TABLE OF CONTENTS

SECTION **PAGE**

LIST OF FIGURES

FIGURE **PAGE**

SECTION A1
INTRODUCTION

A1.1 SCOPE

Appendix A1 contains definitions for the various Unified Capabilities (UC) systems, subsystems, and components, along with acronyms and abbreviations used within the entire Unified Capabilities Requirements 2010~~08~~ (UCR ~~2008~~2010).

A1.2 APPENDIX A1 OVERVIEW

This appendix consists of four sections as follows:

- Section A1 describes the scope of this appendix.
- Section A2 contains a glossary describing the terminology used within the UCR 2010.
- Section A3 lists the abbreviations and acronyms used within the UCR 2010.
- Section A4 contains the references used within the UCR 2010.

THIS PAGE INTENTIONALLY LEFT BLANK

SECTION A2
GLOSSARY AND TERMINOLOGY DESCRIPTION

A2.1 OVERVIEW

This glossary defines terms as they apply to the UCR 2010. It is understood that other documents or organizations may define the terms differently. These terminology definitions are not requirements and are defined to provide context for a requirement in the UCR 2010.

A B C D E F G H I J K L M N O P Q R S T U V W

A

Add-On Transfer and Conference Calling A feature set that provides the user with the capabilities to handle more than one call at a time on a given line.

Admission Control The process by which flows are allowed to enter a network based on their level of quality of service.

Aggregate Service Class An aggregation of service classes based on a selected set of quality of service criteria.

Appliance A hardware platform with its supporting software that performs a single function or multiple functions.

Application Layer Control Protocol See Call Control.

Approved Products List (APL) A list of products that have received Joint Interoperability Certification (JIC) and Information Assurance Accreditation (IAA) from the Defense Information System Network (DISN) Designated Approval Authorities (DAAs) in accordance with the Department of Defense Instruction (DoDI) 8100.3. The list is published on the Joint Interoperability Test Command (JITC) home page (http://jitc.fhu.disa.mil/tssi/apl.html).

Approved Products List System Under Test (SUT) The set of appliances required to meet a Defense Switched Network (DSN) switch certification (i.e., multifunction switch (MFS), end office). Examples of a SUT include Time Division Multiplexing (TDM) or circuit switch components, Voice over Internet Protocol (VoIP) system components (e.g., Local Session Controller (LSC) and gateway), local area network (LAN) components (e.g., routers and Ethernet switches), and end instruments.

Assured Forwarding (AF) Provides delivery of Internet Protocol (IP) packets in four independently forwarded AF classes. Within each AF class, an IP packet can be assigned one of three different levels of drop precedence. In case of congestion, the drop precedence of a packet determines the relative importance of the packet within the AF class. A congested Differentiated Services (DS) node tries to protect packets with a lower drop precedence value from being lost by preferably discarding packets with a higher drop precedence value. A DS node must allocate forwarding resources (i.e., buffer space and bandwidth) to AF classes so that, under reasonable operating conditions and traffic loads, packets of an AF class x do not have a higher probability of timely forwarding than packets of an AF class y if x is less than y. [RFC 2597]

~~**Assured Real Time Services (ARTS) Softswitch (SS)** The ARTS SS within the DoD environment is defined in accordance with the International Softswitch Consortium definition and is a programmable network appliance that provides the following capabilities:~~

- ~~Controls connection services for a media gateway and/or native IP end points.~~
- ~~Selects processes and services that can be applied to a call.~~
- ~~Provides routing for call control within the network based on signaling and customer database information.~~
- ~~Transfers control of the call to another network element.~~
- ~~Interfaces to and supports management functions such as provisioning, fault, and billing.~~
- ~~Ability to control the access of sessions within and external to its domain.~~

~~In the fiscal year (FY) 2008 architecture, the ARTS SS is not a standalone appliance and its functionality is included within the functions of a multifunction softswitch (MFSS). The FY 2012 architecture may support a standalone ARTS SS. To support these capabilities, the ARTS SS includes a Local Session Controller (LSC), Media Gateway Controller (MGC), and signaling gateway. In addition to the International Softswitch Consortium definition, the ARTS SS is also capable of policing subtended LSCs, ARTS SSs, and MFSSs, and performing preemption in the Defense Information Systems Network (DISN) wide area network (WAN) between itself and other MFSSs or SSs using the WAN Level Assured Services Admission Control (W-ASAC).~~

Assured Service The ability of a system to optimize session completion rates for all IMMEDIATE/PRIORITY (I/P) users despite degradation because of network disruptions, natural disasters, or surges during crisis or war.

Assured Services Admission Control (ASAC) A process by which the quality of service requirements of a higher precedence service will be met at the expense of a lower precedence service if the network conditions do not allow meeting quality of service requirements of all services.

Assured Services Local Area Network (ASLAN) The Internet Protocol (IP) network infrastructure components used to provide command and control voice services to end users. It applies to switch certifications for Multifunction Switches, End Office Switches, Small End Office Switches, and Private Branch Exchange 1, and to certifications for Local Session Controllers, Multifunction Softswitches, and Softswitches. A local area network that supports IMMEDIATE/PRIORITY (I/P) users is considered an ASLAN. The ASLAN has two configurations depending on whether it supports I/P users or FLASH/FLASH OVERRIDE (F/FO) users. An ASLAN that supports I/P users is classified a Medium Availability ASLAN and the primary requirements that differentiate it from a non-ASLAN are that it requires a 2-hour power backup capability for all ASLAN components in addition to providing 0.99997 reliability. An ASLAN that supports F/FO users is classified a High Availability ASLAN and the primary requirements that differentiate it from a Medium Availability ASLAN are that it requires an 8-hour power backup capability for all ASLAN components in addition to providing 0.99999 reliability.

Assured Services Session Initiation Protocol (AS-SIP) A session signaling protocol consisting of a defined set of Session Initiation Protocol signaling standards and incorporating DoD Assured Service functionality.

Assured Services Session Initiation Protocol (AS-SIP) End Instrument (AEI) A user appliance that interacts with an associated serving appliance using the AS-SIP to originate, accept, and/or terminate a voice, video, and/or data session(s).

Assured Services Session Initiation Protocol (AS-SIP) Signaling Appliance Any DoD signaling appliance (exclusive of end instruments) that supports the receipt, processing, or forwarding of AS-SIP messages. These appliances MAY support the receipt and forwarding of encapsulated Integrated Services Digital Network User Part (ISUP) Multipurpose Internet Mail Extension (MIME) objects.

Audio Add-On A feature that allows a participant to join a videoconference via audio (telephone) only.

Automated Receiving Devices (ARD) A family of automated devices, which are customer premises equipment or network elements, that attaches to the receiving end of a telephone call. Typical ARDs will have an automatic call distribution front-end, which could be as simple as a queue that handles incoming calls on a first come first serve basis. More complex ARDs can be full function Automatic Call Distributors that also include predetermined schemes and route calls

based on routing criteria and, quite often, database handling instructions. Once in queue, if the call is not answered in a specified amount of time and the caller had not terminated the call, ARD can terminate the call or send the call to another location. Usually the ARD invokes a network carrier-based "take back and transfer" to the alternative location. Automated Receiving Devices do not originate calls to the network.

Availability The fraction of the time the system is available to a service user's requests. The time during which the system is unavailable is called downtime; the time during which the system is available is called uptime. In Internet Protocol (IP) terms, it is the percentage of time that the packet loss is less than the threshold. [~~NCID v3 QoS (T300~~GESP~~)~~]

B

Back-to-Back User Agent (B2BUA) "A back-to-back user agent (B2BUA) is a logical entity that receives a request and processes it as a user agent server (UAS). In order to determine how the request should be answered, it acts as a user agent client (UAC) and generates requests. Unlike a proxy server, it maintains dialog state and must participate in all requests sent on the dialogs it has established. Since it is a concatenation of a UAC and UAS, no explicit definitions are needed for its behavior." [RFC 3261]

Blocking The process by which a message is denied entry to a network that is caused by a lack of resources in the network.

C

Call A message that is subject to Call Admission Control or Session Admission Control. A Voice over Internet Protocol (IP) or Video over IP call that is placed or answered by a Proprietary End Instrument or Assured Services Session Initiation Protocol (AS-SIP) End Instrument end user.

Call Admission Control (CAC) A process in which a call is accepted or denied entry (blocked) to a network based on the network's ability to provide resources to support the quality of service requirements for the call.

Call Connection Agent (CCA) The CCA is part of the Session Control and Signaling functions and includes both the Interworking Function and the Media Gateway Controller. As a result, the scope of the CCA includes the following areas:

- Control of Assured Services Session Initiation Protocol (AS-SIP) sessions within the network appliance

- Support for public switched telephone network (PSTN) and Voice over IP (VoIP) signaling protocols

- Protocol interworking of signaling protocols (for example, AS-SIP ⇔ DoD Common Channel Signaling System No. 7 interworking) through the CCA IWF control of Media Gateways that link the network appliance with Time Division Multiplexing network elements

- Support for interactions with other network appliance functions

- Support for assured ~~real time~~ services ~~(ARTS)~~ voice ~~calls~~ and ~~ARTS~~ video calls

- Support for assured services ~~ARTS~~ user features and services

Call Control Establishes, modifies, and terminates sessions (e.g., multimedia conferences). It can invite participants to existing sessions, such as multicast conferences. [Referred to as Application Layer Control Protocol in RFC 3261.]

Call Forwarding Variable This feature allows ROUTINE precedence calls attempting to terminate to a line to be redirected to another customer-specified line served by the same office or by another office for Defense Switched Network and/or commercial.

Call Hold A feature that provides the capability for the user to hold a call for an extended period, and then return to the call, with or without making another call.

Call Stateful A proxy is call stateful if it retains state for a dialog from the initiating INVITE to the terminating BYE request. A call stateful proxy is always transaction stateful, but the converse is not necessarily true. [RFC 3261]

Call Waiting A feature whereby a line in the talking state is alerted by a call waiting tone when another call is attempting to complete to that line. The call waiting tone is only audible to the line with the Call Waiting feature activated. Audible ringing is returned to the originating line.

Cancel Call Waiting A feature that allows the customer with Call Waiting service to inhibit the operation of call waiting for one call.

Certificate Path A sequence of certificates that connect the target certificate to one of the relying party's trust points. Construction of the path is known as path development and

verification of that path provides a chain of trust and is known as path processing. A target certificate belongs to an end-entity that either sent a signed message to the relying party or to which the relying party desires to send an encrypted message. This is also called a certificate chain.

Certificate Trust List (CTL) A predefined list of items that have been signed by a trusted entity. All items in the list are authenticated and approved for use by the signing entity.

Chat The capability for two or more users operating on different computers to exchange text messages in real time. Chat is distinguished from instant messaging (IM) by being focused on group chat, or room-based chat. Typically, room persistence is a key feature of multiuser chat; in contrast with typically ad hoc IM capabilities.

Circuit Emulation Service (CES) over Internet Protocol (IP) Circuit Emulation Service over IP is trunking of time division multiplexing (TDM) data between IP points. Circuit Emulation Service over IP provides a method to transport T1/E1 or T3/E3 streams over an IP network. The service is similar to CES over asynchronous transfer mode (ATM) that has been in the industry for some time but the transport layer is IP. The circuit may include compression, which may include silence suppression, and echo cancellation. The CES over IP is also known as Circuit Emulation Service over Packet.

Classifier An entity that selects packets based on the content of packet headers according to defined rules. [RFC 2475]

codec Acronym for Coder/Decoder. In video teleconferencing, an electronic device that converts analog signals, typically video and/or voice, into digital form and compresses them into a fraction of their original size to save frequency bandwidth on a transmission path. The device also multiplexes digital data, such as graphic images into the transmitted signal. It also performs the inverse operation; decompressing received signals, demultiplexing them, and converting previously digitized analog signals nearly back to their original state.

Common Channel Signaling System No. 7 (i.e., SS7 or CCS7) A global standard for telecommunications defined by the International Telecommunications Union (ITU) Telecommunication Standardization Sector (ITU-T). The standard defines the procedures and protocol by which network elements in the Public Switch Telephone Network (PSTN) exchange information over a digital signaling network to effect wireless (cellular) and wire line call setup, routing, and control. The ITU definition of SS7 allows for national variants, such as the American National Standards Institute and Telcordia Technologies standards used in North America, and the European Telecommunications Standards Institute standard used in Europe.

Community of Interest (COI) The COI is a switch-based feature as opposed to a network-wide feature, i.e., no COI information is transported between switches. Calls are defined as being internal to the COI if:

1. For an outgoing call request, the dialed destination matches a code in the user's COI screening list.

2. For local calls only, an incoming call request is to a user who is assigned to the same COI group as the calling user.

All other local calls to/from a COI member, including incoming interswitch call requests received via trunk facilities, are treated as external calls to the COI. Call requests received via incoming trunk facilities are deemed external but these do not undergo any COI screening; and hence, are not subject to the special COI restrictions and privileges.

Community of Interest (COI) Group A feature that enables users to form groups, to and from which access is subject to special restrictions and privileges. A COI group consists of a COI screening list, a COI precedence level, and COI group classmarks.

Community of Interest (COI) Group Classmarks Specify the outgoing and incoming call restrictions and/or privileges for calls internal to the COI group. The COI group classmarks are defined as follows:

1. COI Outgoing Classmarks. A COI group user with no outgoing classmarks limits the COI user to making calls, which are internal to the COI only, i.e., to only those destination codes that are specified within the COI screening list. The user is allowed to exercise the normal authorized precedence for these calls.

2. Outgoing Precedence Allowed. The COI user is allowed to exercise up to and including the COI precedence for calls internal to the COI.

3. Outgoing Precedence Mandatory. Only COI precedence calls are permitted for calls internal to the COI.

4. Outgoing Calls Barred within the COI. This restriction means that a COI user cannot make calls to destination codes specified in the COI screening list.

Community of Interest (COI) Incoming Classmarks A COI group user with no incoming classmarks limits the COI user to receiving locals from members of those COIs of which the user is a member. All other local calls are restricted. There is no restriction on calls received over trunk facilities because these do not undergo COI screening.

1. Incoming Precedence Mandatory. This COI service only permits calls internal to the COI that are at the COI precedence level, which only applies for local calls that are internal to the COI (i.e., if the local calling user is a member of those COIs of which the user is a member).

2. Incoming Calls Barred within the COI. This restriction means that a COI user cannot receive calls from members of those COIs of which the user is a member. Unless the member classmark incoming access option is applied, calls from other non-COI members or other COI members are restricted also.

3. COI Member Classmarks. In addition to the COI group classmarks that are part of the COI group, specific COI members can have COI classmarks at the subscriber level that specify the type of incoming and outgoing call restrictions and/or privileges for calls external to the COI.

Community of Interest (COI) Member A user that has a COI group assigned is defined as being a member of that COI group.

Community of Interest (COI) Outgoing Access Allows a COI user to make calls external to the COI, i.e., to all other destination codes not specified in the COI screening list (i.e., external to the COI). The user is only allowed to exercise the normal authorized precedence level for these calls.

Community of Interest (COI) Precedence Level A COI feature that allows the precedence level to be required or allowed, depending up the COI group classmarks, for calls to/from users of a COI group.

Community of Interest (COI) Screening List A COI feature that allows a list to be specified for individual destinations or codes representing groups of destinations. Each code in this list can be from 3 to 15 digits. Outgoing calls are screened against this list together with the COI group classmarks to allow or deny the call request.

Conditional Requirement [Conditional] A requirement that addresses features and capabilities that are not considered critical for DoD mission support based on DoD policies. However, it is recognized that such features and capabilities do have utility for some users or for specific operations. To ensure interoperability and consistency of these features and capabilities across all platforms, these features and capabilities are specified with set parameters. If these features and capabilities are provided, the appliance shall perform and meet the specifications as identified in the appropriate section of UCR 2010~~, Change 1~~.

Conditional – Deployable A variation of the "Conditional" case, where the requirement is Required for Fixed appliances, such as Local Session Controllers (LSCs) and Multifunction

Softswitches in Fixed DoD networks, but is Conditional for Deployable appliances, such as LSCs in Deployable DoD networks. In other words, "Conditional – Deployable" means "Required for Fixed appliances, but Conditional for Deployable appliances."

Conference Calling A feature that allows the user to establish a call involving up to six conferees (including the user).

Congested Condition One hundred percent utilization of bandwidth on the link, or links, under test. Link traffic may be any combination of real time services traffic and data, up to and including specified traffic engineering (i.e., 25 percent voice, 25 percent video, and data up to 100 percent).

Control Plane Quality of service mechanism to provide the ability to route data correctly and perform actions during session establishment and operation to allow a network to meet quality of service needs in the data plane. The purpose of this plane is to define the configuration, start-up conditions, and instability conditions of the control protocols, which may include routing protocols, multicast protocols, link management, and Multiprotocol Label Switching protocols.

Converged All types of services, defined by the ~~Net-Centric Implementation~~GIG Enterprise Service Profile Document (~~NCID~~GESP), ~~Version 2 (NCIDv2) Quality of Service (QoS) T300~~, exist simultaneously on the same Internet Protocol (IP) network.

Converged Local Area Network (CLAN) A local area network (LAN) is an Internet Protocol (IP) network, composed of routers and LAN switches, that is used to connect nodes that are geographically close, usually within the same building. In a wider view of a LAN, multiple LANs are interconnected in a geographically compact area, usually by attaching the LANs to a higher speed local backbone called a campus area network (CAN). A CAN is larger than a LAN but smaller than a metropolitan area network (MAN) or wide area network (WAN). A CLAN is a LAN that supports multiple types of IP services. In the DoD, the CLAN supports voice, video, and data services as a minimum. The CLAN is not intended to support IMMEDIATE/ PRIORITY (I/P) users and the requirements associated with a CLAN are those that are typical for commercial real time service CLANs to include commercial grade power and availability requirements.

Converged Network An Internet Protocol (IP) network used to transmit a combination of voice, video, and/or data services.

Cryptographic Boundary An explicitly defined continuous perimeter that establishes the physical bounds of a cryptographic module and contains all the hardware, software, and/or firmware components of a cryptographic module.

Cryptographic Module The set of hardware, software, and/or firmware that implements approved security functions, including cryptographic algorithms and key generation, and are contained within the cryptographic boundary.

Customer Edge Router (CE Router) A router located at the boundary between the Edge segment and the Access segment of the wide area network. The CE Router provides traffic conditioning, bandwidth management on a granular service class (i.e., voice, video) basis, and quality of service using per hop behaviors. A base/post/camp/station may have a single CE Router or multiple CE Routers based on the local architecture.

D

Data Plane Quality of service mechanism to provide the ability to manage and forward data packets, including one or more of the following: packet marking and re-marking, implementing scheduling and packet drop priorities, metering the traffic and performing congestion control, and policing and shaping the traffic. The purpose of this plane is to define the configuration, start-up conditions, and instability conditions of the data traffic including the traffic, collection of network elements, links between network elements, and interface profile.

Default Best Effort (BE) This is the common, best-effort forwarding behavior available in existing routers. When no other agreements are in place, it is assumed that the packets belong to this aggregate. Such packets may be sent into a network without adhering to any particular rules, and the network will deliver as many of these packets as possible and as soon as possible, subject to other resource policy constraints. This forwarding behavior is not be used for VoIP.

Defense Switched Network (DSN) An interbase, nonsecure or secure DoD telecommunications system that provides dedicated telephone service, voice band data, and dial-up video teleconference for end-to-end command use and DoD authorized IMMEDIATE/PRIORITY (I/P) and non-I/P users in accordance with national security directives. Nonsecure dial-up voice (telephone) service is the system's principal service.

Denied Originating Service A system feature that provides the capability to deny call originations selectively to individual lines.

Deployable Voice Exchange (DVX) A tactical switch with military-unique features capabilities to support the assured service requirements of Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6215.01C used for rapid deployment situations and contingencies in the deployable environment. The DVXs can either be DVX Commercial Off-the-Shelf (COTS) (DVX-C), or DVX legacy (DVX-L) tactical (TRI-TAC) systems. Normally, a DVX is connected to the DSN using gateway trunks routed through a Standard Tactical Entry Point/Teleport location. It can be connected directly to the DSN (Tandem Switch/Multifunction Switch/End Office/Small End Office), if it is to be used as a temporary solution for either of the following:

- An initial capability that will be replaced by a more permanent solution for sustainment of strategic operations.

- A solution for augmenting a strategic communications facility to meet rapid growth or restoration requirements.

Deployable Voice Exchange Commercial Off-the-Shelf (DVX-C) A Government-deployable commercial switch that may have been modified for use within deployable environments to provide military-unique features.

Deployable Voice Exchange – Legacy (DVX-L) A Government-deployable legacy voice switching system, such as the Common Baseline Circuit Switch and Unit Level Circuit Switch.

Deployable Private Branch Exchange (PBX) A PBX that is allowed to connect to the Defense Switched Network via a Standard Tactical Entry Point/Teleport. Deployed PBX Type 1s do not tandem calls and are not approved to support FLASH and FLASH OVERRIDE users as their only means of communication. FLASH and FLASH OVERRIDE users shall be supported by other means such as a long local.

Differential Treatment A mechanism that allows differential handling of packets in the Edge and Core nodes. It also includes providing differential treatment at the time of resource reservation and provisioning requests.

Differentiated Services (DS) A quality of service delivery model, in which the flows are classified, policed, marked, and shaped at the edges of a DS domain. The nodes in the core of the network handle packets according to the per-hop behavior that is selected based on the contents of the DS field (Differentiated Services Code Point) in the packet header.

Differentiated Services Architecture Contains two main components. One is the fairly well understood behavior in the forwarding path and the other is the more complex and still emerging background policy and allocation component that configures parameters used in the forwarding path. The differentiated services architecture is based on a simple model where traffic entering a network is classified and possibly conditioned at the boundaries of the network, and assigned to different behavior aggregates. Each behavior aggregate is identified by a single Differentiated Services Code Point. Within the core of the network, packets are forwarded according to the per-hop behavior associated with the DSCP. [RFC 2475]

Differentiated Services (DS) Field (DSField) The six most significant bits of the Internet Protocol, version 4, Type of Service octet or the Internet Protocol, version 6, traffic class octet.

Differentiated Services Code Point (DSCP) A value that is encoded in the Differentiated Services field and that each DS node must use to select the per-hop behavior that is to be experienced by each packet it forwards.

Directed Inward Dial (DID) A feature that allows an incoming call to reach a specific Private Branch Exchange (PBX) station line without attendant assistance. With DID, the switch seizes a DID trunk and outpulses the station line number to the PBX. If the called station's line is idle and not restricted from receiving terminating calls, the PBX alerts the called station and returns audible ringing on the incoming connection. If the called station's line is busy, the PBX returns busy tone. If the called station is restricted from receiving terminating calls, the PBX routes the incoming call to an announcement, reorder tone, or to the attendant.

Disruptive A disruptive action is one that prevents a given quantity of end instruments from placing or receiving a session for more than 5 minutes.

Directed Call Pickup A feature that permits a user to dial a code and station number and pick up a call that has been answered or is ringing at another telephone, provided the rung telephone permits dial pick-up.

DoD Directives Broad DoD policy documents containing what is required by legislation, the President, or the Secretary of Defense to initiate, govern, or regulate actions or conduct by the DoD Components within their specific areas of responsibilities.

DoD Secure Communications Devices (DSCD) Hardware devices that, when placed in the secure mode, protects the transmission of classified voice, data, or facsimile over the Defense Switched Network or other connected networks to another compatible DSCD. Examples of DSCDs include, but are not limited to, Secure Terminal Equipment, Secure Telephone Unit – Third Generation (STU-III), plus the Omni and Sectera Wireline Terminals, secure Global System for Mobile, and other like devices, including wireless devices.

E

Edge Boundary Controller (EBC) An appliance that provides voice and/or video ~~RTS~~ firewall functions. The EBC is located at the boundary between the Edge Segment and the Access Segment. The EBC is a logical entity and its functionality may be implemented in one or more physical platforms. The EBC is used to exert control over the signaling and media streams and is involved in setting up, conducting, and tearing down sessions. Edge Boundary Controllers are put into the signaling and/or media path between the calling and the external called party. The effect of this behavior is that not only the signaling traffic, but also the media traffic (i.e., voice, video) crosses the EBC. Ultimately, EBCs allow their owners to control the kinds of session that can be placed through the networks on which they reside, and overcome some of the problems

that firewalls and Network Address Translation cause for Internet Protocol real time service sessions. As a minimum, the EBC provides topology hiding, "pinholing," and filtering.

Edge Label Switch Router (eLSR) The eLSR provides the edge function of multiprotocol label switching (MPLS). The eLSR is where the label is first applied when traffic is directed toward the core of the MPLS network or last referenced when traffic is directed toward the customer. The eLSR functions as an MPLS provider edge (PE) node in an MPLS network. The eLSR is a functional PE that sends traffic to provider nodes to traverse the MPLS core, and it sends traffic to the customer interface known in MPLS terminology as the customer edge. The eLSR uses IP routing toward the customer interface and "label swapping" toward the MPLS core. The term label edge router is used interchangeably with eLSR.

Elastic Service A service that has high tolerance for packet loss, delay, and jitter (i.e., delay variation) at packet and overall message level. This service can tolerate a wide variation in the throughput.

Emergency Service A feature that provides a 3-digit universal telephone number (911) that gives the caller access to help and support from an emergency service bureau.

Encapsulated Time Division Multiplexing (TDM) T1/E1 or Fractional T1/E1 encapsulated within an alternate transport mechanism that provides assured bandwidth for both signaling and bearer channels.

End Instrument (EI) An EI is a user appliance that initiates, accepts, and/or terminates a voice or video session. End instruments may be stand-alone applications or may be used in conjunction with other applications (e.g., softphone). They may provide a single service (e.g., voice or video) or multiple services (e.g., videophone). In addition, EIs may signal the Local Session Controller with standardized protocols or proprietary protocols.

The EI is the primary user interface to customers for voice or video and is the originating or terminating endpoint for all voice or video sessions. It is the appliance at which the user assigns the precedence to the voice or video session, and the EI is responsible for collecting and disseminating the user authentication information to the LSC. Finally, the EI is the point at which the network level Class of Service markings are set based on instructions from the LSC.

End Office (EO) A central office at which user lines and trunks are interconnected, providing long-distance service by interconnecting with Defense Switched Network (DSN) nodal switches. End Office switches provide users with switched call connections and all DSN service features, including Multilevel Precedence and Preemption.

A switch which is integral to the DSN and serves as a primary switch for long distance services for either an installation or group of installations in a geographic area by interconnecting users to the DSN nodal switches.

End Terminal (ET) Optical terminal capable of terminating up to 80 channels in one direction.

Entity An appliance or human that uses the system.

Expedited Forwarding (EF) The forwarding treatment for a particular Differentiated Services (DS) aggregate where the departure rate of the aggregate's packets from any DS node must equal or exceed a configurable rate. The EF traffic should receive this rate independent of the intensity of any other traffic attempting to transit the node. If the EF Per Hop Behavior is implemented by a mechanism that allows unlimited preemption of other traffic (e.g., a priority queue), the implementation shall include some means to limit the damage EF traffic could inflict on other traffic (e.g., a token bucket rate limiter). Traffic that exceeds this limit shall be discarded. [RFC 3246]

Explicit Routing In explicit routing, the entire list of nodes traversed by the label switched path is specified in advance. The path specified could be optimal or not, but is based on the overall view of the network topology and, potentially, on additional constraints. This is called constraint-based routing. Along the path, resources may be reserved to ensure quality of service. This permits traffic engineering to be deployed in the network to optimize use of bandwidth.

F

Fiber Maintenance Margin The additional margin allocated to the fiber network to warrantee the continuous operation to the end of life of the Dense Wave Division Multiplex (DWDM) system. This Fiber Maintenance Margin does not include any margins for DWDM seller's equipment.

Fiber Span The span loss is the attenuation between Dense Wave Division Multiplex (DWDM) equipment at adjacent DWDM locations (i.e., Optical Line Amplifier (OLA), Reconfigurable Optical Add Drop Multiplexer (ROADM), and End Terminal). The span loss consists of the outside plant (OSP) loss, the intraoffice loss, and the fiber maintenance margin. The OSP loss is the loss from Fiber Service Delivery Point (FSDP) to FSDP. The intraoffice is from FSDP to DWDM equipment as illustrated in Figure A-1. The entrance/exist points of the DWDM equipment are the reference points MPI-S/R according to ITU-T Recommendation G.692.

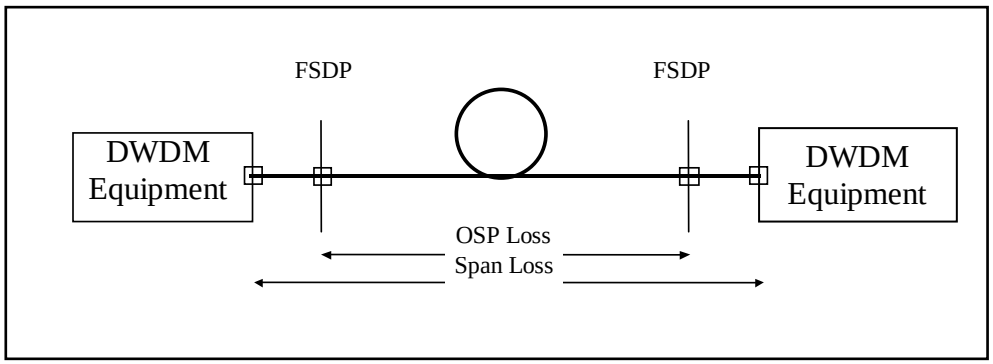

Figure A-1. Difference between OSP Loss and the Span Loss

Fixed Wireless End Instrument (WEI) Those WEIs that access a single wireless LAN access system (WLAS) for the duration of the session and are not expected to traverse between WLASs so that handoffs are required.

FLASH and FLASH OVERRIDE Users A special class of users who have access to the Defense Switched Network for "essential communications for planning, directing, and controlling operations of assigned forces pursuant to assigned missions. This user requires capabilities that provide crises, pre-attack, and theater non-nuclear war telecommunications service for intelligence, alert, and strategic readiness." This user also requires communications among the President, Secretary of Defense, Chairman of the Joint Chiefs of Staff, and other members of the Joint Chiefs of Staff, Service Chiefs, and the Combatant Commanders.

Flow A group of packets with similar attributes as defined by a subset of the parameters in the Internet Protocol (IP) header of each packet (see Microflow).

Forward Equivalence Class (FEC) Each multiprotocol label switching router independently selects the next hop for a given FEC. An FEC describes a group of packets of the same type; all packets assigned to an FEC receive the same routing treatment. An FEC can be based on an IP address route or the service requirements for a packet, such as low latency.

Future Narrowband Digital Terminal/Secure Communications Interoperability Protocol (FNBDT/SCIP) A protocol used to conduct a secure session with another FNBDT/SCIP capable device. SCIP and FNBDT are synonymous terms and refer to the protocols currently documented in the SCIP series of documents (e.g., SCIP-215, 216.). The current preference is to use SCIP because it more accurately reflects a protocol (layer 7) as opposed to the use of FNBDT, which implies a terminal type.

G

Granular Service Class Represents the atomic identification of a service class. A set of granular service classes, sharing similar traffic characteristics form an aggregate service class.

Guaranteed Service The use of signaling to reserve network resources end-to-end to meet preset performance objectives.

H

H.323 to H.320 Gateway A videoconferencing end point that converts between H.323 IP end point protocols and services and H.320 end point protocols and services for transport of videoconferencing data between IP and serial or integrated services digital network (ISDN) sessions.

I

INTERMEDIATE/PRIORITY (I/P) Users INTERMEDIATE/PRIORITY users include any person (regardless of the position in the chain-of-command) who issues or receives guidance or orders that direct, control, or coordinate any military forces regardless of the nature of the military mission (including combat support, administration, and logistics), whether said guidance or order is issued or effected during peacetime or wartime.

In-band Term used when network management system connects to the network device using the same Ethernet port communication channel used for user traffic.

Incoming Access Allows a community of interest (COI) user to receive local calls from all other non-COI user and from those other COI users who allow outgoing access.

Incoming Access with Precedence Allows a community of interest (COI) user to receive only local COI precedence level calls from all other non-COI users and from those other COI users who allow outgoing access.

Individual Line A line arranged to serve only one main station, although additional stations may be connected to the line as extensions of the main station.

Inelastic Service A real time service that typically requires strict bounds on packet loss, delay, and jitter. It cannot tolerate throughput variations based on network load level. In this architecture, a Circuit Emulation, commonly identified as a mechanism, has been included in this category to meet special DoD messaging requirements.

Information Assurance (IA) Enabled Product A system whose primary function is not IA, but does have some IA functions.

Information Assurance (IA) Product A system that provides IA functions consistent with the IA services and categories (i.e. authentication, confidentiality). An IA product's primary purpose is to provide IA functions.

Information Technology (IT) Products Systems that receive, process, store, display, or transmit DoD real time services.

Instant Messaging (IM) The capability for users to exchange one-to-one ad hoc text messages over a network in real time. IM is not the same as and must not be confused with signaling or equipment messaging; IM is always user generated and user initiated.

Integrated Access Switch (IAS) Customer premise equipment system that interconnects a Defense Switched Network (DSN) switch and terminal equipment (TE), such as inverse multiplexers, routers, video teleconferencing (VTC) codecs, VTC monitors, and multipoint control units (see Figure A-2, Typical Connections for an IAS). The IAS is able to originate multiple data and/or video calls according to the worldwide numbering and dialing plan (WWNDP). Depending on the local implementation, primary rate interface (PRI) to PRI, PRI to basic rate interface (BRI), or BRI to PRI, interconnection is accomplished by the IAS. The IAS does not possess any functions of multilevel precedence and preemption (MLPP), but is able to originate calls that can be interpreted by the DSN switch as precedence calls and may be preempted on the DSN switching platforms and network trunks (see FigureA-3, MLPP Implementation and the IAS). The IAS is be provisioned so the number of provisioned TE interface bearer channels do not exceed the number of provisioned DSN or commercial interface bearer channels. This is to reduce the possibility of a call destined for a TE from being blocked by the DSN or commercial interfaces on the IAS not having available bearer channels for this call. It should also be noted that VTC call inherently has a ROUTINE precedence level.

The IAS is able to originate multiple data and/or video calls in accordance with the WWNDP, as described in UCR ~~2010~~2008, Section 5.2.3.5.1, DSN Worldwide Numbering and Dialing Plan. Depending on the local implementation, PRI to PRI, PRI to BRI or BRI to PRI, interconnection is accomplished by the IAS. The IAS does not possess any functions of MLPP, but shall be able to originate calls that can be interpreted by the DSN switch as precedence calls and may be preempted on the DSN switching platforms and network trunks (see Figure A-3, MLPP Implementation and the IAS).

The IAS shall be provisioned so that the number of provisioned TE interface bearer channels shall not exceed the number of provisioned DSN or commercial interface bearer channels. This is to reduce the possibility of a call destined for a TE from being blocked by the DSN or

commercial interfaces on the IAS not having available bearer channels for this call. It should also be noted that VTC call inherently has a ROUTINE precedence level. A typical layout of the IAS is illustrated in Figure A-2, Typical Connections for an IAS.

Figure A-4, Applications for the IAS, shows the applications for the IAS.

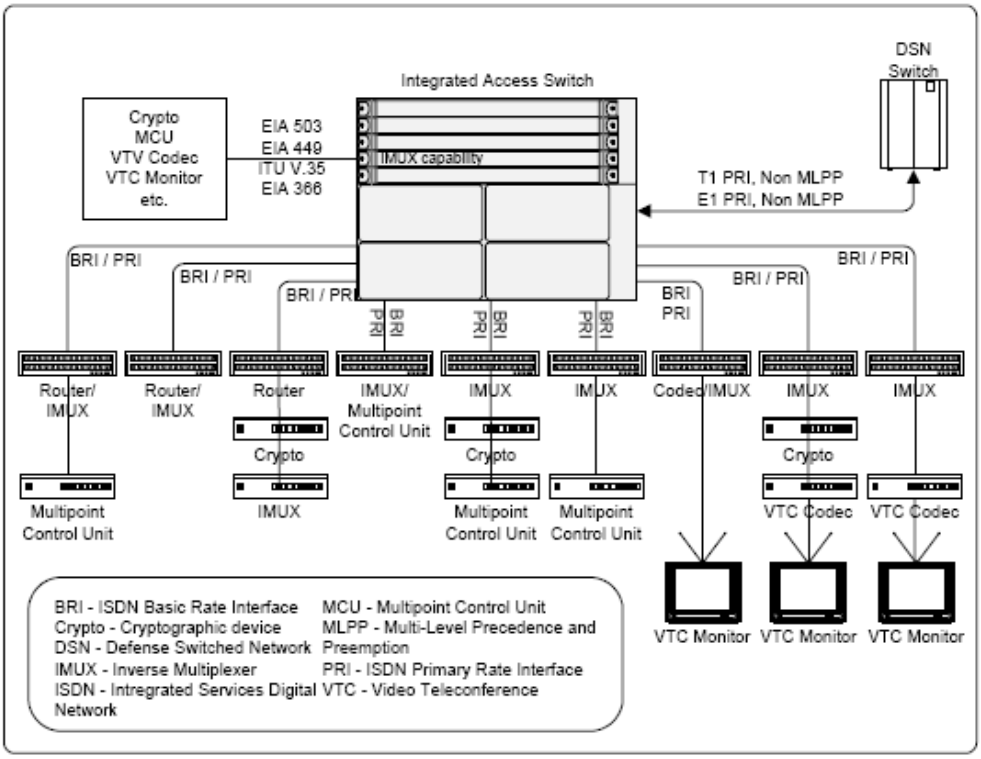

Figure A-2. Typical Connections for an IAS

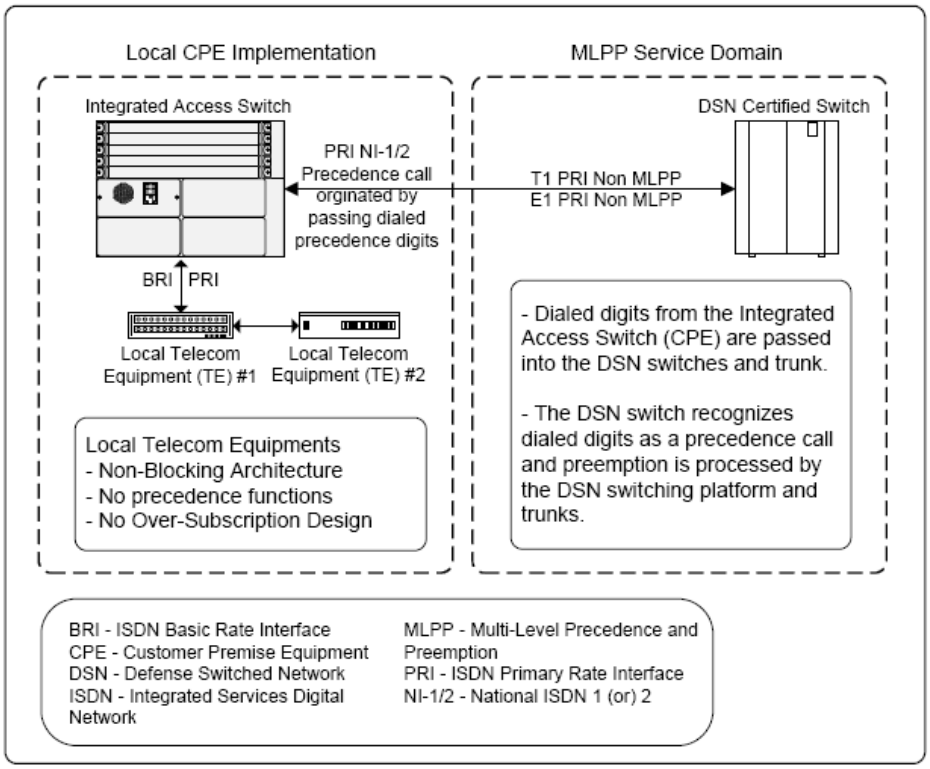

Figure A-3. MLPP Implementation and the IAS

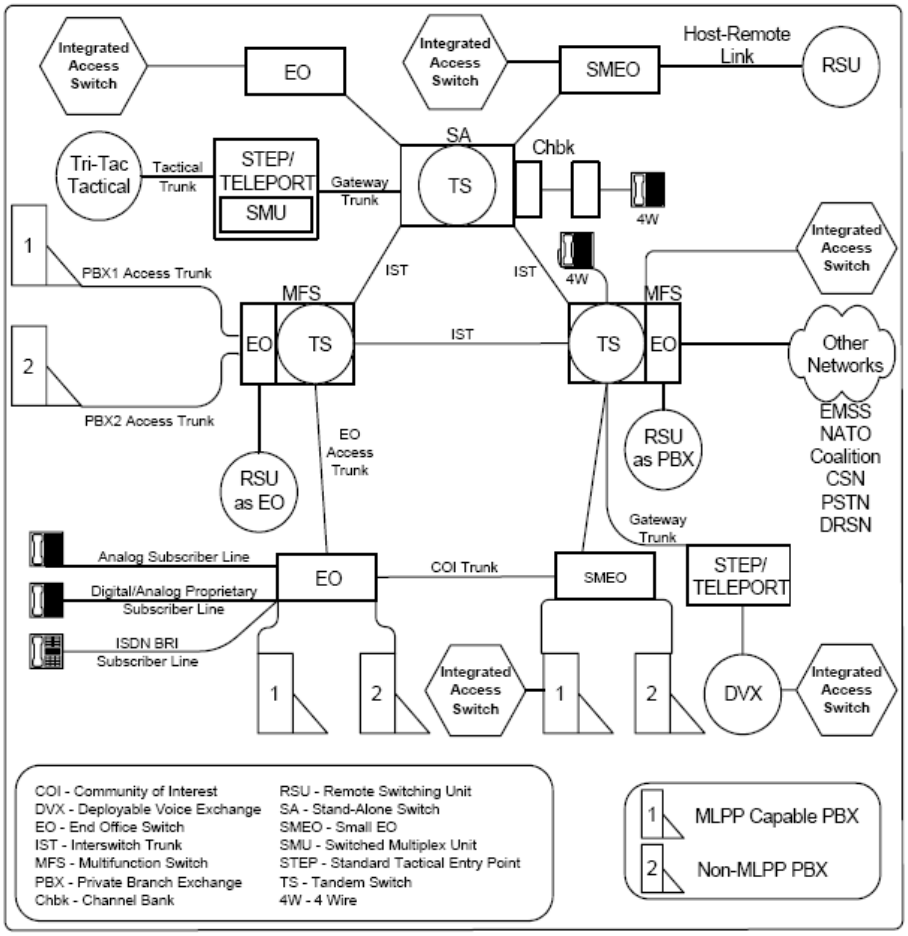

Figure A-4. Applications for the IAS

Integrated Services Digital Network (ISDN) Devices An ISDN specifies a number of reference points that define logical interfaces between functional ISDN devices such as terminals, terminal adapters, network termination devices, and line termination equipment. ISDN specifies a number of reference points that define the interconnection of these devices.

Integrated Services Digital Network devices are defined as:

TE1 Terminals with built-in ISDN connection capability (also referred to as TE).

TE2 An existing terminal device, designed for existing protocols. It is not capable of directly interoperating with ISDN.

TA An adaptive device designed to permit TE2s to interoperate with ISDN.

Integrated Services Digital Network (ISDN) Integrated Access Interface An ISDN user-network interface in which the interface structure is composed of multiple B-channels and one D-channel.

Integrated Services Digital Network (ISDN) NT 1 A single (physical) layer device that contains all the necessary interface elements to communicate with the network. It terminates the local loop and provides the user interface to the network while isolating this user from the operation of the network.

Integrated Services Digital Network (ISDN) R The reference point representing a standardized non-ISDN interface, such as Electronics Industries Alliance (EIA)-232, EIA-422, V.24, V.35, and others. The combination of a Terminal Adapter and Terminal Equipment Type 2 is equivalent to a Terminal Equipment Type 2.

Integrated Services Digital Network (ISDN) Reference Points The reference points applicable for Defense Switched Network customer premises equipment are as follows:

U The reference point for a Basic Rate Interface (BRI) connection between a local loop and a customer premise. The U interface specifies a single pair loop over which a logical 4-wire circuit is derived.

S The reference point between ISDN user terminal equipment (i.e., Terminal Equipment Type 1 (TE1) or Terminal Adapter (TA)) and the network termination equipment (NT1). This is a 4-wire interface that supports the BRI 2B+D protocol.

R The reference point representing a standardized non-ISDN interface such as Electronics Industries Alliance (EIA)-232, EIA-422, V.24, V.35, and others. The combination of a TA and Terminal Equipment Type 2 (TE2) is equivalent to a TE1.

Integrated Services Digital Network (ISDN) S The reference point between ISDN user terminal equipment (i.e., Terminal Equipment Type 1 or Terminal Adapter) and the network termination equipment (NT1). This is a 4-wire interface that supports the Basic Rate Interface 2B+D protocol.

Integrated Services Digital Network (ISDN) Terminal Adapter An adaptive device designed to permit Terminal Equipment Type 2 to interoperate with ISDN.

Integrated Services Digital Network (ISDN) Terminal Eequipment (TE) 1 Terminals with built-in ISDN connection capability (also referred to as TE).

Integrated Services Digital Network (ISDN) Terminal Eequipment (TE) An existing terminal device designed for existing protocols. It is not capable of directly interoperating with ISDN.

Integrated Services Digital Network (ISDN) U The reference point for a Basic Rate Interface connection between a local loop and a customer premise. The U interface specifies a single pair loop over which a logical 4-wire circuit is derived.

Internet Protocol (IP) Centric Internet Protocol centric architectures are designed around an IP core packet switching system. These solutions have distributed IP devices that function together to provide voice and video over IP services.

Internet Protocol (IP) Data Subscriber A user connected to an IP network to receive Department of Defense IP services, such as data and IP video. Defense Switched Network IP telephony is not included.

Internet Protocol (IP) Enabled An approach that utilizes traditional time division multiplexing (TDM) circuit switches that offer Voice over IP (VoIP) at a line-side instrument. This solution has a TDM circuit switch as the core device with VoIP being provided as a line function similar to other analog or digital telephony instruments. The requirements of the UCR 2010~~, Change 1~~, Section 5.2, for nonsecure or secure voice, data, video teleconferencing, and fax are met primarily via the circuit switch portion. The Defense Switched Network interface requirements (i.e., T1/E1) are provided via the circuit switch and the connectivity to the IP local area network is via Ethernet. Internet Protocol-enabled architectures can be certified for Private Branch Exchange through Multifunction Switch applications.

Internet Protocol Packet Delay Variation (IPDV) The one-way IPDV(n) is defined as the difference between the one-way delay of the selected packet and the packet with the lowest IP Packet Transfer Delay (IPTD) in the evaluation interval: IPDV(n) = IPTD(n) – IPTD(0). [ITU-T Y.1540, IETF RFC 3393]. In the case of real time services, the measurements are typically taken at the end instruments. This is also referred to as jitter.

Internet Protocol Packet Loss Ratio (IPLR) A metric measured for packets traversing the network segment between the source reference point and destination reference point. The IPLR metric is reported as the number of lost packets at the destination reference point divided by the number of packets sent at the sender reference point to that destination. [ITU-T Y.1540, IETF RFC 2680]. This is also referred to as packet loss.

Internet Protocol Packet Transfer Delay (IPTD) The single instance of the one-way IPTD measurement is defined as the time the test packet traverses the network segment(s) between two reference points. The metric is defined as a time starting from the time the first bit of the packet is put on the wire at the source reference point to the time the last bit of the packet is received at the receiver reference point. [ITU-T Y.1540, IETF RFC 2679] In the case of real time services, the measurement points are the end instruments. This is also referred to as latency.

Internet Protocol Signaling Gateway (IPSG) Function A signaling appliance that relays, translates, or terminates IP messages between various IP signaling protocols such as Assured Service Session Initiation Protocol, H.323, H.248, and IP proprietary signaling protocols.

Internet Protocol (IP) Telephony Subscriber A Defense Switched Network INTERMEDIATE/PRIORITY (I/P) or non-I/P user that receives voice service via an IP telephone instrument (also known as an End Instrument).

Internet Protocol (IP) Transport The aggregation of various types of IP traffic, such as voice, video, and data, and that is transmitted over IP link(s).

Internet Protocol Version 6 (IPv6) Capable A system or product capable of receiving, processing, and forwarding IPv6 packets and/or interfacing with other systems and protocols in a manner similar to that of IP version 4 (IPv4).

Internet Protocol Version 6 (IPv6) Capable Networks Networks that can receive, process, and forward IPv6 packets from/to devices within the same network and from/to other networks and systems, where those networks and systems may be operating with only Internet Protocol version 4 (IPv4), only IPv6, or both IPv4 and IPv6.

Internet Protocol Version 6 (IPv6) Capable Products Products (whether developed by commercial vendor or the Government) that can create or receive, process, and send or forward (as appropriate) IPv6 packets in mixed Internet Protocol version 4 (IPv4)/IPv6 environments.

Internet Protocol Version 6 (IPv6) Enabled Network An IP network that is supporting operational IPv6 traffic through the network end-to-end.

Internet Protocol (IP) Video Subscriber A Defense Switched Network non-IMMEDIATE/ PRIORITY user that receives video service via an IP video system.

J

Jitter The one-way jitter is defined as the difference between the one-way delay of the selected packet and the packet with the lowest IP Packet Transfer Delay (IPTD) in the evaluation interval: IPDV(n) = IPTD(n) – IPTD(0). [ITU-T Y.1540, IETF RFC 3393]. In the case of real time services, the measurements are taken at the end instruments. This is also referred to as the IP Packet Delay Variation (IPDV).

K

KG-194/194A (National Security Agency cryptographic device nomenclature) A Federally-certified cryptographic device used to provide data encryption at data rates from 9.6 kilobits per second (kbps) up to 13 megabits per second (Mbps) over synchronous serial links, typically on dedicated circuit networks.

KIV-7/KIV-7HS (National Security Agency cryptographic device nomenclature) A Federally-certified cryptographic device used to provide data encryption at data rates up to 2.04 8 megabits per second (Mbps) over synchronous serial links on dial-up and other nondedicated networks.

KIV-19/19A (National Security Agency cryptographic device nomenclature) A Federally-certified cryptographic device used to provide data encryption at data rates from 9.6 kilobits per second (kbps) up to 13 megabits per second (Mbps) over synchronous serial links on dedicated circuit or dial-up network paths. The KIV-19/19A is interoperable with the KG-194/194A.

L

Label Header created by an Edge Label Switch Router and used by Label Switch Routers to forward packets. The header format various based on the network media type. In the Assured Services Local Area Network environment, the header is a "shim" located between the Layer 2 and Layer 3 headers.

Label Distribution Protocol (LDP) This protocol defines a set of procedures used by multiprotocol label switching (MPLS) routers to exchange label and stream mapping information. It is used to establish label switched paths (LSPs), mapping routing information directly to Layer 2 switched paths. It is also commonly used to signal at the edge of the MPLS network the critical point where non-MPLS traffic enters. For example, such signaling is required when establishing MPLS virtual private networks.

Label Edge Router (LER) The LER provides the edge function of Multiprotocol Label Switching (MPLS). The LER is where the label is first applied when traffic is directed toward the core of the MPLS network or last referenced when traffic is directed toward the customer. The LER functions as an MPLS provider edge (PE) node in an MPLS network. The LER is a functional PE that sends traffic to provider nodes to traverse the MPLS core, and it sends traffic to the customer interface known in MPLS terminology as the customer edge. The LER uses IP routing toward the customer interface and "label swapping" toward the MPLS core. The term label edge router edge (eLSR) is used interchangeably with LER.

Label Information Base (LIB) As the network is established and signaled, each multiprotocol label switching router builds a LIB, a table that specifies how to forward a packet. This table associates each label with its corresponding Forward Equivalence Class and the outbound port to forward the packet to. Typically, the LIB is established in addition to the routing table that traditional routers maintain.

Label Swapping A forwarding decision process set that allows streamlined forwarding of data by using labels to identify classes of data packets, which are treated indistinguishably when forwarding.

Label Switch Router (LSR) or Label-Switching Router (LSR) The LSR provides the core function of multiprotocol label switching. The LSR is equipped with both Layer 3 routing and Layer 2 switching characteristics. The LSR functions as a provider node in an Multiprotocol Label Switching network.

Label Switched Path (LSP) Multiprotocol label switching networks establish LSPs for data crossing the network. An LSP is defined by a sequence of labels assigned to nodes on the packet's path from source to destination. An LSP directs packets in one of two ways: hop-by-hop routing or explicit routing. The path goes through one or more label switch routers at one level of the hierarchy followed by a packet in a particular Forward Equivalence Class.

Latching The ability of the Reconfigurable Optical Add Drop Multiplexer to maintain its current state in the event of power failure.

Latency The single instance of the one-way latency measurement is defined as the time the test packet traverses the network segment(s) between two reference points. The metric is defined as a time from the time the first bit of the packet is put on the wire at the source reference point to the time the last bit of the packet is received at the receiver reference point. [ITU-T Y.1540 and IETF RFC 2679] In the case of real time services, the measurement points are typically the end instruments; also referred to as IP packet transfer delay (IPTD).

Link The communications facilities between adjacent nodes of a network. For voice over IP systems, a link is an Ethernet connections used for IP transport as opposed to trunks used for time division multiplexing (TDM) transport.

Link Pair To ensure no single point of failure to more than 64 Internet Protocol (IP) telephony subscribers, IP network links shall have a second link (standby or load sharing). The combination of the two links is called a link pair.

Local Area Network (LAN) Access or Edge Layer The point at which local end users are allowed into the LAN. In addition, these layers may use access lists or filters to further optimize

the needs of a particular set of users. This term should not be confused with the wide area network (WAN) Edge or WAN Access Layer.

Local Area Network (LAN) Core Layer A high-speed switching backbone and is designed to switch packets as fast as possible within the LAN. This term should not be confused with the wide area network (WAN) Core Layer.

Local Area Network (LAN) Distribution or Building Layer The distribution or building layer of the LAN is the demarcation point between the access and core layers, and helps to define and differentiate the core. The purpose of this layer is to provide boundary definition and is the place at which packet manipulation can take place.

Local Area Network (LAN) Network Links Internal Internet Protocol (IP)/Ethernet links that interconnect LAN components.

Local Area Network (LAN) Switch A LAN switch is an appliance that reduces contention on LANs by reducing the number of nodes on a segment using microsegmentation techniques. On a microsegmented network, a LAN segment may have many nodes or a single node. The LAN switch handles all the connections between nodes on different LAN segments when they need to communicate through an internal matrix switch that processes the packets at the Media Access Control (MAC) layer. When a packet arrives at the switch, its destination MAC address is quickly noted and a connection is set up to the appropriate end segment. Subsequent packets are relayed through the switch without the need to store and forward packets, as is necessary with bridges. Many LAN switches in the DoD Internet Protocol Real Time Services architecture include router functions.

Local Session Controller (LSC) A call stateful Assured Service Session Initiation Protocol (AS-SIP) signaling appliance at a base/post/camp/station that directly serves Internet Protocol (IP) end instruments (EIs). The LSC MAY consist of one or more physical platforms. On the trunk side, the LSC employs AS-SIP signaling. On the line side, the LSC may serve any combination of Session Initiation Protocol EIs, H.323 EIs, and proprietary EIs. The LSC MUST be an intermediary for every inbound and outbound call signaling message received and transmitted by each IP EI served by the given LSC.

Local Session Controller (LSC) Level Assured Services Admission Control (L-ASAC) The processes on an LSC that ensure that quality of service requirements of a higher precedence service will be met at the expense of a lower precedence service if the network conditions do not allow meeting quality of service requirements of all services. The processes are typically associated with the preemption of lower precedence sessions to an end instrument to ensure that higher precedence sessions can be completed.

Location Server The purpose of the location server is to provide information on call routing and called address translation (where a called address is contained within the called Session Initiation Protocol Secure (SIPS) Uniform Resource Identifier (URI) in the form of the called number). The service provided by the server is typically referred to as location services. The Call Connection Agent (CCA) uses the routing information stored in the location server

- to route internal calls from one Local Session Controller (LSC) end instrument (EI) to another EI on the same LSC,
- to route outgoing calls from an LSC EI to another LSC, a multifunction softswitch (MFSS), or a time division multiplexing (TDM) network, and
- to route incoming calls from another LSC, an MFSS, or a TDM network to an LSC EI or MFSS.

Long Local A long-local telephone is connected remotely through an assured transmission means, time-division multiplexing (TDM) or Internet Protocol, to a distant site. This interface is handled as a local loop to the host Defense Switched Network switch.

M

Management Plane A quality of service mechanism to access network elements for network management purposes, such as provisioning and policy setting. This plane is used to define the configuration, startup conditions, and instability conditions of the management protocols and features including Simple Network Management Protocol, Logging/Debug, statistics collection, and management configuration sessions such as telnet, Secure Shell, and serial console.

Mean Time Between Failures (MTBF) For a particular interval, the total functional life of a population of an item divided by the total number of failures (requiring corrective maintenance actions) within the population.

Mean Time To Repair (MTTR) The total amount of time spent performing all corrective maintenance repairs divided by the total number of those repairs.

Measurement-Based Admission Control An approach that bases a call control decision on the monitoring of network capacity. Admits, rejects, or redirects calls based on current network congestion.

Media Gateway (MG) A MG within the DoD environment is defined in accordance with the Internet Engineering Task Force Request for Comments 2805 and provides the media mapping and/or transcoding functions between Time Division Multiplexing (TDM) and Internet Protocol

(IP) networks. The MG terminates switched circuit network (SCN) facilities (e.g., trunks, loops), packetizes the media stream, if it is not already packetized, and delivers packetized traffic to an IP network. It would perform these functions in the reverse order for media streams flowing from the IP network to the SCN.

Media Gateway Controller (MGC) The function in a signaling appliance that controls a media gateway.

Media Server A platform in an Internet Protocol (IP) telephony network that transmits dial tones, busy signals, and announcements.

Meet-Me Conferencing A conference that is established when each conferee dials into the conference bridge at a scheduled time as directed by a conference attendant.

Message A unit of data transfer from an application in one host to an application in another host.

Message Discrimination and Distribution Function A function that examines the Destination Point Code of a received signaling message to determine whether or not it is destined to the receiving signaling point.

Metering The process of measuring the temporal properties (e.g., rate) of a traffic stream selected by a classifier. The instantaneous state of this process may be used to affect the operation of a marker, shaper, or dropper, and/or may be used for accounting and measurement purposes. [RFC 2475]

Metric A quality of service delivery parameter such as delay, packet loss, data rates, availability, etc.

Microflow A single instance of an application-to- application flow of packets that is identified by source address, source port, destination address, destination port, and protocol identification. [RFC 2475]

Minimum Requirements Features and capabilities considered necessary for a particular switch type to support warfighter missions in the DoD. These features and capabilities will require certification prior to introduction into the Defense Switched Network.

Mobile Code Software modules obtained from or provided by remote systems, transferred or downloaded across a network, and then executed on local systems without explicit installation or execution by the recipient.

Modem over IP (MoIP) The transport of modem data across an Internet Protocol network, via either modem relay or voiceband data (modem pass-through) techniques.

Modem Relay A subset of Modem over IP in which modem termination is used at gateways, thereby allowing only the baseband data to reach the packet network.

Multicasting The ability of the Reconfigurable Optical Add Drop Multiplexer to allow one input wavelength to be duplicated on multiple output tributary and line ports.

Multifunction Softswitch (MFSS) A network appliance that provides the following functions:

- Provides all multifunction switch (MFS) functions:
  - Tandem Switch
  - End Office
  - Softswitch functions
  - Global directory services
  - Local Session Controller (LSC) functions
  - Media gateway functions
  - Signaling gateway functions
  - Network management
  - Fault, configuration, accounting, performance, and security

- Supports Policy Based Network Management:
  - Assured Services Admission Control budget controls
  - Customer Edge Routerqueue bandwidth allocations
  - End instrument (EI) session origination control (according to designated groups)
  - EI session destination control (according to designated groups)

The MFSS is a logical entity and its functionality MAY be implemented in one or more physical platforms.

The MFSS is an MFS that is enhanced with an Internet Protocol (IP) interface. As with any MFS, the MFSS supports End Office and Tandem Switch capabilities. In addition, the MFSS also includes LSC and Assured ~~Real Time~~ Services (A~~RT~~S) Softswitch (SS) functions to support line-side IP EI and trunk-side Assured Service Session Initiation Protocol (AS-SIP) and AS-SIP for Telephones signaling. For Tandem Switch EIs connected to the MFSS, the MFSS is the media end point for sessions connected to an IP EI at the terminating location.

Multifunction Switch (MFS) "A switch that combines the tandem function of the SA [Stand-Alone] switch with the EO [End Office] function of connecting the user's lines to the backbone trunks. Logically the SA and EO are separate, but within the same physical configuration." [CJCSI 6215.01C]

Multilevel Precedence and Preemption (MLPP) In circuit-switched systems, a priority scheme:

- For assigning one of several precedence levels to specific calls or messages so that the system handles them in a predetermined order and timeframe,
- For gaining controlled access to network resources in which calls and messages can be preempted only by higher priority calls and messages,
- That is recognized only within a predefined domain, and
- In which the precedence level of a call outside the predefined domain is usually not recognized.

Multilevel Precedence and Preemption (MLPP) Call A call that has a precedence level established and is either being set up or is set up. In Digital Subscriber Signaling System No. 1 (DSS1: ISDN Q.931 signaling), an MLPP call is a call from an MLPP subscriber for which a setup has been sent but no DISCONNECT has been sent or received.

Multilevel Precedence and Preemption (MLPP) Service Domain A set of MLPP subscribers (MLPP users) and the network and access resources that are in use by that set of MLPP subscribers at any given time. Connections and resources that are in use by MLPP subscribers may be preempted only by higher precedence calls from MLPP subscribers within the same domain. The service domain consists of a 3-octet field ranging from 00 00 00 to FF FF FF in hexadecimal. The Defense Switched Network service domain is zero (0).

Multipoint Control Unit (MCU) An end point that enables intercommunication of three or more video teleconferencing (VTC) end points in a conference call. It can be used with two VTC end points, e.g., while beginning or ending a multipoint conference. The MCU may perform mixing or switching of audio, video, and data.

N

Nailed Up Connections A special use permanently established path through a switch for either a network circuit (trunk) or a special service facility.

Network All telecommunications equipment that has any part in processing a call or a supplementary service for the user referred to. It may include local exchanges, transit exchanges, and Network Termination 2 (NT2) but does not include the integrated services digital network (ISDN) terminal and is not limited to the “public” network or any other particular set of equipment.

Network Domain A contiguous set of network elements that belongs to the same administrative authority.

Network Element (NE) A component of a network through which the Defense Switched Network (DSN) bearer and/or signaling traffic transits. For Internet Protocol (IP) transport, the IP connection may transit a Local Area Network (LAN), Metropolitan Area Network (MAN), Campus Area Network (CAN), or Wide Area Network (WAN) dependent on its deployment. Network elements may include multiplexers, routers, Channel Service Units/Digital Service Units (CSU/DSUs), compression devices, circuit emulation, channel banks and/or any network device that could have an effect on the performance of the associated network traffic. The network diagram, shown in Figure A-5, Network Element Diagram, shows the typical network element as a stand-alone device or integrated into the transmission interfaces of switches or other network devices. The use of NEs shall not provide the means to bypass the DSN as the first choice for all switched voice and dial-up video telecommunications between DoD user locations.

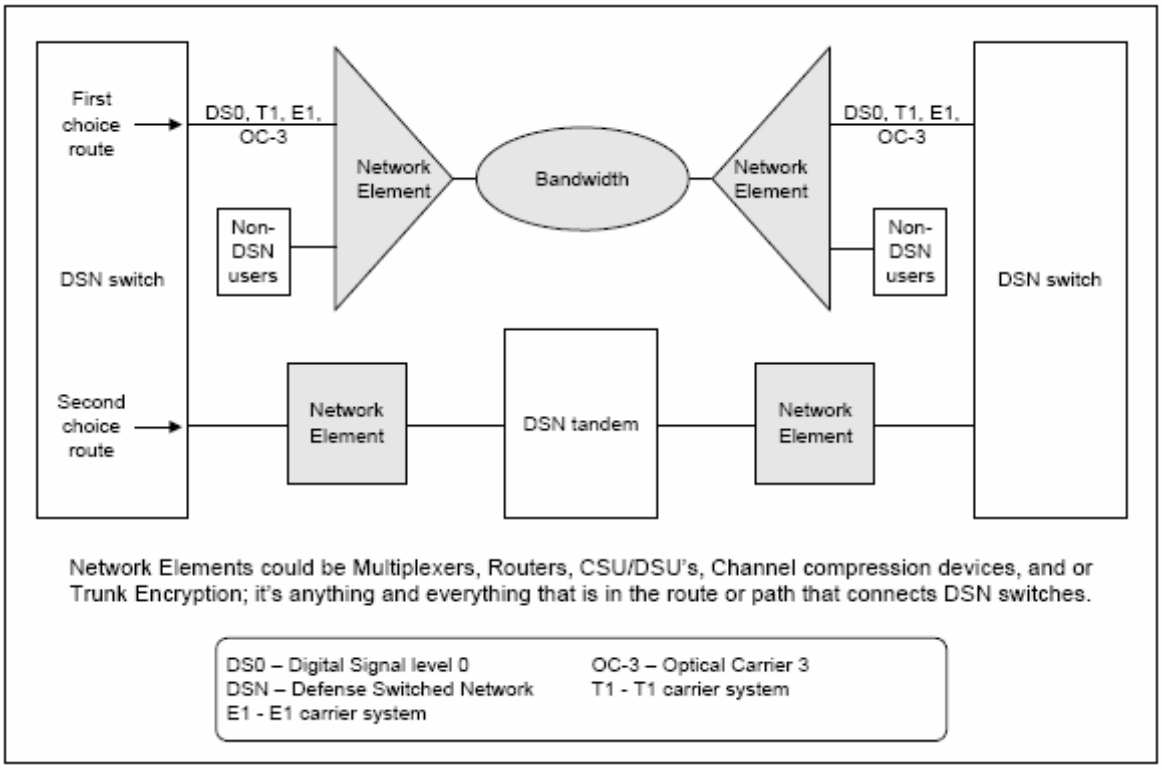

Figure A-5. Network Element Diagram

Network Signaling Based Admission Control Determines based on requests indicated through a signaling protocol whether a node or network has sufficient available resources to meet the requested quality of service. [RFC 2205]

New Call The event that precipitates a trunk seizure or when preemption for reuse of a trunk is used to support multilevel precedence and preemption (MLPP) calls in the Defense Switched Network.

Nomadic Wireless End Instrument (WEI) Those WEIs that are mobile and may traverse different wireless local area network (LAN) access systems during a single session.

Non-Assured Service Local Area Network (Non-ASLAN) The Internet Protocol (IP) network infrastructure components used to provide services (i.e., voice, video, and data) to end users. Non-ASLANs are "commercial grade" and provide support to C2 (ROUTINE only calls) (C2(R)) or non-C2 voice subscribers.

Non-Assured Voice Audio sessions that are established independent of any call admission control exercised by a Local Session Controller.

Non-Assured Video Video sessions that are established independent of any call admission control exercised by either a Local Session Controller or H.323 Gatekeeper.

Non-Blocking Local Area Network (LAN) A LAN that is provisioned so all Internet Protocol (IP) telephone instruments can be off hook simultaneously and successfully engaged in a full duplex voice call.

Non-Command and Control (C2) Users Those users, DoD, non-DoD, non-U.S. Government and foreign government users that have no missions or communications (equipment) requirements to originate or receive C2 communications under the existing military scenarios. These users are provided access to the Defense Switched Network (DSN) for economic benefit of the DoD. During a crisis or contingency, these users may be denied access to the DSN. It is the primary means of secure (Secure Telephone Unit, Third Generation (STU-III)/Secure Terminal Equipment (STE) family) communications for non-tactical C2 users. The DSN must be the user's first choice; however, if the DSN is not immediately available, or if the called party does not have access to DSN service, other long-distance calling methods may be used.

Non-Converged Network A network that is used solely to provide Defense Switched Network Voice over Internet Protocol (IP) services. A separate IP network will be used to provide IP data services.

Non-Preemptive Service A Global Information Grid service that offers a committed information rate between two or more Edge networks, where the bandwidth cannot be preempted for the use of any other party than the one contracting for the service.

Non-Signaled Flow A flow that does not require signaling to enter a network.

O

Objective Requirement [Objective] A requirement that does not have to be met in the initial operational capability (IOC), but must be met in the final operational capability (FOC). The time frame associated with the IOC is fiscal year (FY) 2008 and the time frame associated with the FOC is FY 2012 unless specifically stated.

Offered Load Control A mechanism that allows control of packet transfer loads to keep them within specified bounds (possibly described in Service Level Agreements) so that network domains can deliver the promised quality of service.

Operations, Administration, and Maintenance (OA&M) A set of network management functions, providing network fault indication, performance information, and data and diagnosis functions.

Optical Line Amplifier (OLA) Provides optical signal reamplification without converting to electrical signal along the spans between optical terminal equipment.

Originating Internet Protocol (IP)/Time Division Multiplexing (TDM) Signaling Gateway Function The function related to receiving an Initial Address Message (IAM) from the Signaling System No. 7 network and generating an Assured Service Session Initiation Protocol INVITE with the encapsulated Integrated Services Digital Network User Part (ISUP) IAM that is sent over the IP network – identical to Outgoing Interworking Unit in International Telecommunications Union – Telecommunication Standardization Sector Recommendation Q.1912.5, "Interworking between Session Initiation Protocol (SIP) and Bearer Independent Call Control Protocol or ISDN User Part."

Originating Gateway An Assured Service Session Initiation Protocol for Telephones signaling appliance performing the originating Internet Protocol (IP)/Time Division Multiplexing (TDM) signaling gateway function.

Outgoing Call Trace A feature that allows the tracing of nuisance calls to a specified directory number suspected of originating from a given local office. The tracing is activated when the specified directory number is entered. A printout of the originating directory number, outgoing trunk number, or terminating number, and the time and date is generated for every call to the specified directory number.

Out-of-Band A term used to describe network management systems that connect to the network device using a physically separated network from the network used for user traffic. This requires an additional network infrastructure to support management traffic.

Outside Plant (OSP) Loss The OSP loss is measured from the fiber connector in the Fiber Service Delivery Point (FSDP) of a Dense Wave Division Multiplex (DWDM) equipment location to the fiber connector (at the other end of the fiber) in the FSDP of the next DWDM equipment location. The OSP loss is the combined loss of the fiber attenuation itself and the attenuation due to splices and connectors across the span.

Overflow Process A process that allows calls of a lower precedence level and narrower calling area to utilize unused calling capacity of a higher precedence level and equal and wider calling area, and equal precedence level and wider calling area call types without blocking calls of a higher precedence level and wider calling area.

P

Packet Loss A metric measured for packets traversing the network segment between the source reference point and destination reference point. The Packet Loss metric is reported as the number of lost packets at the destination reference point divided by the number of packets sent at the sender reference point to that destination. [ITU-T Y.1540, IETF RFC 2680]. This is also referred to as Internet Protocol Packet Loss Ratio.

Packet Marking Marking in packets following their classification for a given service delivery; which includes Differentiated Services Code Point, Flow Label, or Security Parameter Index bit fields.

Path Communications link between two network components. A path may include a number of communications links.

Per-Domain Behavior (PDB) An externally observable edge-to-edge functional and performance quality of service behavior on a per-domain basis.

Per-Hop Behavior (PHB) An externally observable forwarding behavior applied at a Differentiated Services (DiffServ)-compliant node to a DiffServ behavior aggregate based on the DiffServ Code Point marking in the packet. [RFC 2475]

Policing The process of discarding packets (by a dropper) within a traffic stream in accordance with the state of a corresponding meter enforcing a traffic profile. [RFC 2475]

Precedence The designation assigned to a message by the originator to indicate its relative level of importance of the message up to the originator's maximum authorization level as defined by DoD requirements documents.

Precedence-Based Assured Service (PBAS) This service implies that, in general, quality of service requirements of a higher precedence class will be met at the expense of a lower precedence class if the network conditions do not allow meeting quality of service requirements of all service classes.

Precedence Based Treatment The process of allocating network resources to the higher-precedence messages more favorably while restricting lower-precedence traffic during periods of resource shortage.

Precedence Inversion The phenomenon that occurs when a higher precedence flow or flow aggregate does not receive its quality of service commitments, while a lower-precedence flow or flow aggregate competing for the same communications source does receive its quality of service commitments.

Precondition "A precondition is a set of constraints about the session that are introduced in the offer. The recipient of the offer generates an answer, but does not alert the user or otherwise proceed with session establishment. That only occurs when the preconditions are met. This can be known through a local event (such as a confirmation of a resource reservation), or through a new offer sent by the caller." [RFC 3312]

Preemptable Circuit A circuit that is active with or reserved for a multilevel precedence and preemption (MLPP) call: (a) within the same domain as the preempting call and (b) with a lower precedence than the preempting call. A busy or reserved circuit for which a precedence level has not been specified is not a preemptable circuit.

Preemption Initiating Exchange An exchange that is congested (i.e., no idle circuits) and has received a preempting call setup.

Preferred Elastic A specially created service class category to meet unique DoD application requirements; it has varying degrees of service class categories. Examples include short, interactive transactions and delay-sensitive file transfers.

Presence/Awareness A status indicator that conveys ability and willingness of a potential user to communicate. A user's client provides presence information (presence state) via network connection to a presence service, which is stored in what constitutes the user's personal availability record (called a presentity) and can be made available for distribution to other users (called *watchers*) to convey the user's availability for communication. Presence information has wide application in many communication services and is one of the innovations driving the popularity of instant messaging (IM) or recent implementations of voice over IP clients.

A user client may publish a presence state to indicate its current communication status. This published state informs others that wish to contact the user of the user's availability and

willingness to communicate. The most common use of presence is to display a status indicator icon on IM clients, and a list of corresponding text descriptions of each of the states. Even when technically not the same, the "on-hook" or "off-hook" state of a called telephone is an analogy; the caller receives a distinctive tone indicating unavailability ("line busy") or availability ("ring-back tone" followed by voice mail).

Private Branch Exchange (PBX) PBX Line A line appearance at the local switching system that permits connection to a customer premise switching system. The connecting facility may be 1- or 2-way, and it may be loop start or ground start. A PBX line is like an individual line except for ringback, power cross test, and permanent signal treatment.

Private Branch Exchange (PBX) Type 1 (PBX1) A PBX with multilevel precedence and preemption (MLPP) capabilities. Based on mission requirements, this switch may serve those non-command and control (C2) users defined as DoD users having a military mission that might receive C2 calls for orders or direction at precedence levels above a ROUTINE precedence, even though they do not have a C2 mission for issuing guidance or orders. FLASH and FLASH OVERRIDE users are not authorized to be served by a PBX1 and must connect to an End Office Switch or a Small End Office Switch.

Private Branch Exchange (PBX) Type 2 (PBX2) A PBX with no multilevel precedence and preemption (MLPP) capabilities. This switch can serve only DoD, non-DoD, non-governmental, and foreign government users having no missions or communications requirement to ever originate or receive command and control (C2) communications under existing military scenarios. These users are provided access to the DSN for the economic or policy benefits of the DoD, when it is not in conflict with local Public Telephone and Telegraph (PTT) ordinances. During a crisis or contingency, they may be denied access to the Defense Switched Network. The IMMEDIATE/PRIORITY, FLASH, and FLASH OVERRIDE users are not authorized to be served by a PBX2.

Propagation Delay Travel time of an electromagnetic signal from one measurement point to another.

Proprietary End Instrument (PEI) A user appliance that interacts with the serving appliance (i.e., Local Session Controller, Multifunction Softswitch, or Wide Area Network Softswitch), using a proprietary protocol to originate, accept, and/or terminate a voice, video, or data session(s).

Proprietary IP Trunk (PIPT) A virtual network element that provides a virtual IP trunk connection between a pair of certified switches (e.g., Deployable Voice Exchange (DVX) to DVX, DVX to Private Branch Exchange Type 1 (PBX1), DVX to Private Branch Exchange Type 2 (PBX2)). The PIPT may use proprietary signaling but must support the equivalent

features and functions of a Primary Rate Interface, multilevel precedence and preemption (MLPP) (T1.619a), or non-MLPP (NI 1/2), as appropriate.

Protection A preplanned alternate path for the service.

Proxy Server "An intermediary entity that acts as both a server and a client for the purpose of making requests on behalf of other clients. A proxy server primarily plays the role of routing, which means its job is to ensure that a request is sent to another entity "closer" to the targeted user. Proxies are also useful for enforcing policy (for example, making sure a user is allowed to make a call). A proxy interprets, and, if necessary, rewrites specific parts of a request message before forwarding it." [RFC 3261]

Q

Quality of Service (QoS) The capability to provide resource assurance and service differentiation in a network. Used with the Local Area Network to provide different priority to traffic flows or sessions, or guarantee a certain level of performance to a traffic flow or session in accordance with requests from the application program. Quality of Service is used in conjunction with traffic tagging to guarantee that prioritized traffic flows or sessions are given preferential treatment.

Quality of Service Domain An administrative network domain that is designed based on a single quality of service architecture and operated under the same set of quality of service policies.

Quality of Service Network A quality of service aware or enabled network; it consists of one or more interconnected quality of service domains.

Queuing Delay Waiting time of a packet for its turn to be serviced at the interface of a network device, such as a router.

R

Reconfigurable Optical Add Drop Multiplexer (ROADM) Optical terminal equipment capable of terminating up to 80 channels in both directions. It performs wavelength add and drop functions, as well as allowing wavelengths to pass through.

Reliability The ability of a system and its parts to perform its mission without failure, degradation, or demand on the support system. See Mean Time Between Failures (MTBF) and Mean Time Between Maintenance (MTBM).

Release to Pivot (RTP) A network routing capability that consists of a collection of call setup procedures that provides flexibility to a Tandem Switch/Multifunction Switch/End Office-type switch to determine conditions for either forwarding a call or releasing it back to a previous switch in the call path. The RTP is a network capability that is invoked in support of service or business needs, and not invoked directly by an end user. The RTP network capability permits an operator services switch, after it has determined a new destination for the call, to have the connection established from the originating switch. The basic capability allows any switch to indicate to switches farther forward in the call path that it has the ability to pivot the call. An application that determines the new destination for the call (in this case, the operator services switch) can release the call then with a Redirection Number parameter containing the address of the new destination. The Pivot switch (in this case, the originating switch) will not terminate the call on receipt of the Release message, but will pass the call forward toward the new destination. The result is that the Release switch, which determined the new destination, saves an incoming and an outgoing trunk relative to the case where the call is forwarded to the new destination.

Remote Switching Unit (RSU) A telecommunications switch that is connected to and dependent upon a host switch (End Office (EO) Switch, Multifunction Switch (MFS), or Small End Office (SMEO) Switch) for some or all centralized operations, administrative, and maintenance capabilities. It is a switching function integral to the Defense Switched Network (DSN) (and part of the Global Information Grid). The RSU may be used to provide different functions: EO/SMEO or Private Branch Exchange (PBX). If used as an EO/SMEO, the RSU must meet all the requirements of an EO/SMEO, and it must be connected via the host-remote link to a DSN backbone Stand-Alone Switch or MFS. If used as a PBX, the RSU must meet all the requirements of a PBX; and it must be connected via a host-remote link to an installation EO/SMEO. Mission requirements of the users connected to the RSU dictate site-specific application as an EO/SMEO or PBX. The RSUs will be tested with and without the host switch for interoperability certification.

Remote Switching Unit (RSU) Degraded Operations The RSU operations when one of two conditions are met: (1) stand-alone, when the host link umbilical has been severed; and (2) partial stand-alone, when the host link umbilical is saturated with traffic or the host link is partially "out-of-service."

Remote Switching Unit (RSU) Normal Operations The RSU operations when the umbilical line or trunk is fully connected to the host switch, and neither the host nor the RSU is in a degraded condition.

Remote Switching unit (RSU) Standalone Operations The RSU operations when the umbilical links between the host and the RSU are completely severe.

Required Requirement [Required] A requirement is required if it must be met in the initial operational capability (IOC). The IOC is associated with the fiscal year 2008 timeframe. An IOC requirement is often labeled a Threshold requirement to differentiate the requirement from an Objective requirement.

Resource Reservation Protocol (RSVP) A protocol developed by the Internet Engineering Task Force for hosts (applications) and routers to communicate service requirements to the network and to enable the routers in the network to set up the reservations.

Response Time Round-trip delay from a network application source through destination, back to the application source.

Restoration The switching of the service to an alternate path after a failure.

Route Code A special purpose Defense Switched Network code that permits the customer to inform the switch of special routing or termination requirements. At the present time, the route code is used to determine whether a call will use circuit-switched data or voice-grade trunking. The route code may be used to disable echo suppressers and cancellers, and override satellite link control.

Router A router is an appliance that is a packet switch that operates at the network layer of the Open Systems Interconnection Protocol model. Routers within the Internet Protocol (IP) Assured~~Real Time~~ Services (A~~RT~~S) architecture interconnect networks over local and wide areas, and provide traffic control and filtering functions when more than one pathway exists between two endpoints on the network. The primary function of routers is to direct IP packets along the most efficient or desired path in a meshed network that consists of redundant paths to a destination. Many routers in the DoD IP UC~~RTS~~ architecture include Local Area Network switch functions and the distinction between the two types of appliances continues to blur.

S

Secure Communications over IP (SCIP) over Internet Protocol (IP) The transport of SCIP information over an IP network. The SCIP traffic can be transmitted over an IP network in many ways, but currently, the U.S. Government requires SCIP devices to support transmission of SCIP on IP networks via V.150.1 Modem Relay.

Secure Cryptographic Processes Secure cryptographic processes constitute the basic requirement for effective data security and effective data protection in the use of information

technology. The basic requirements include digital signatures, authentication and access control, and encryption.

Secure End Instrument (SEI) An end instrument that is able to operate in the normal ~~real time~~assured ~~services (RTS)~~ mode and in a secure (typically type 1 encryption) mode. The primary function of the SEI is to maintain Red/Black separation by applying upstream media encryption for secure calls while maintaining multilevel security filtering to allow a user to talk in either secure or non-secure mode. The Internet Protocol (IP) SEI is not currently designed to support secure video. It is hoped that the Voice over IP secure terminal equipment will adopt the Assured Service Session Initiation Protocol (AS-SIP) as the ~~RTS~~ signaling protocol, which will allow it to interoperate with any AS-SIP-based Local Session Controller. However, it is not known if that capability will be included and the earliest that it might occur is fiscal year 2012. For the purposes of this document, the term end instrument shall apply to an end instrument or SEI unless specifically noted.

Secure Telephone Equipment (STE) This term refers to both a DoD Secure Communications Device (DSCD) and a mode of operation. It is a DSCD that utilizes any one of the multiple supported protocols to conduct a secure session with another compatible protocol device (e.g., Secure Terminal Equipment (STE), Secure Telephone Unit, Third Generation (STU-III), or Future Narrow Band Digital Terminal (FNBDT)/ Secure Communication Interoperability Protocol (SCIP)-capable device).

Secure Telephone Unit (STU) This term refers to both a DoD Secure Communications Device (DSCD) and a mode of operation. A STU has a specific protocol that is used for conducting a secure session with another STU compatible DSCD.

Secure Voice over IP (SVoIP) Provides Type 1 encrypted communications end to end. Security (encryption for confidentiality) is provided at the Application layer using Secure Communication Interoperability Protocol (SCIP) (formerly known as Future Narrow Band Digital Terminal (FNBDT)) devices. The encryption is typically Type 1; however, SCIP/FNBDT devices can use other crypto methods and libraries, such as Advanced Encryption Standard. Secure VoIP provides talker-to-listener security and session unique security levels. It is capable of transitioning through black Public Switch Telephone Network (PSTN) and provides interoperability with legacy service voice systems (Secure Telephone Unit (STU) and Secure Teminal Equipment (STE)).

Secure Voice over Secure IP (SVoSIP) The use of SVoIP devices on a Voice over Secure Internet Protocol (VoSIP) network that provides the following features:

- Security (confidentiality) is provided at both the application and network layers

- Using Secure High Assurance Internet Protocol Encryptor (HAIPES) + Future Narrow Band Digital Terminal (FNBDT)
- Confidentiality within HAIPES domain (end-to-end on top of system high)
- Independent negotiations can permit interoperability with FNBDT only
- HAIPES only systems

Selective Call Forwarding A feature that allows customers to have only calls from selected calling parties forwarded.

Service Class A set of traffic that requires specific delay, loss, and jitter characteristics from the network for which a consistent and defined per-hop behavior applies.

Service Level Agreement (SLA) Binding contractual agreement between two parties, Global Information Grid (GIG) networks service provider and GIG users, listing offered services and service-level specifications regarding the technical parameters of the service requested. An SLA may include traffic conditioning rules. An SLA is often the results of the mission planning process.

Service Level Commitment (SLC) A numerical performance value that specifies a commitment made by the provider to the user, in the service level specifications of the service level agreement.

Service Level Specification (SLS) A set of quantitative performance metrics that together define the service offered to a traffic stream by a Differentiated Services domain related to a specific service level agreement.

Service Provisioning Policy A policy that defines how traffic conditioners are configured on differentiated services (DS) boundary nodes and how traffic streams are mapped to DS behavior aggregates to achieve a range of services. [RFC 2475]

Session The underlying Assured Services Session Initiation Protocol (AS-SIP) or Proprietary Voice over Internet Protocol (VoIP) session that is processed by the Proprietary End Instrument/AS-SIP End Instrument and the Local Session Controller. The VoIP signaling and media streams in the applicance that support an individual end user's call.

Session Initiation Protocol (SIP) The SIP is "…an application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants. These sessions include Internet telephone calls, multimedia distribution, and multimedia conferences." [RFC 3261]

Session Initiation Protocol (SIP) User Agents Intelligent Internet Protocol (IP) telephones with SIP software that create and management a SIP session.

Session Initiation Protocol (SIP) Proxy Server Equivalent to time division multiplexing (TDM) call processing software that detects call for service ("off-hook"), analyzes address digits received, and based on data contained in translation tables/local subscriber line tables obtains the called telephone addressing information. Then it forwards the session invitation directly to the called telephone if it is located in the same domain, or to another proxy server if the call telephone resides in another domain.

Session Initiation Protocol (SIP) Redirect Server Equivalent to time division multiplexing (TDM) routing tables that allow SIP proxy servers to direct SIP session invitations to external domains. The SIP redirect servers may reside in the same hardware as SIP registrar and ISP proxy servers.

Session Initiation Protocol (SIP) Registrar Server Equivalent to time division multiplexing (TDM) subscriber line database tables and classmarks for all telephones served directly off or by the Local Session Controller controlling a domain. In SIP messaging, these servers retrieve and send participant's IP addresses and other pertinent information to the SIP proxy server.

SETUP Message The SETUP message is sent by the calling user to the network or by the network to the called user to initiate call establishment. Defense Switched Network (DSN) calls shall use the SETUP message specified in American National Standards Institute T1.607. The Channel Identification, Calling Party Number (when available), and Called Party Number are mandatory information elements (IEs). For a Multilevel Precedence and Preemption (MLPP) call (invoking MLPP feature) on the DSN user-to-network interface, the SETUP message shall include the Precedence Level IE. It shall contain other IEs, such as the Business Group IE for the Community of Interest feature, when such unique DSN features are required and the call identity IE (as defined in International Telecommunication Union (ITU) Recommendation Q.931) for the MLPP feature. The precedence level and MLPP service domain (both contained in the Precedence Level IE), and the Calling Party Number (contained in the Calling Party Number IE) shall be used to mark the circuit (identified in the Channel Identification IE) to be preempted as "reserved" for reuse by the preempting call when the Look-Ahead for Busy option is exercised on the DSN user-to-network interface.

Seven Digit Dialing The ability to dial using the seven digits of the switch code and line number to establish either interswitch or intraswitch calls within the same numbering plan area.

Shaping The process of delaying packets within a traffic stream to cause it to conform to some defined traffic profile. [RFC 2475]

Signaled Flow A flow that requires signaling to determine if there are sufficient resources to support its quality of service requirements. If the resources do not exist or cannot be preempted, the flow is blocked from entering the network.

Signaling The process of exchanging information between two or more parties to initiate or terminate a communication session, and for the management and maintenance of the session.

Signaling Appliance See Assured Services Session Initiation Protocol (AS-SIP) Signaling Appliance.

Signaling Gateway (SG) Function A signaling gateway function receives/sends switched circuit network native signaling at the edge of a data network. For example, the SG function MAY relay, translate or terminate Signaling System No. 7 (SS7) signaling in an SS7-Internet Gateway. The SG function MAY also be co-resident with the Media Gateway (MG) function to process switched circuit network signaling associated with line or trunk terminations controlled by the MG, such as the D-channel of an Integrated Services Digital Network (ISDN) Primary Rate Interface trunk. The use of the SG function within the Assured Real Time Services Generic System Requirements refers only to SS7 signaling. The use of the SG within the Assured Services Session Initiation Protocol Generic System Specification allows for the SG to be co-resident with the MG. [RFC 2805]

Small End Office (SMEO) "A switch that serves as the primary switch, functions as an EO [End Office], but at smaller DOD [Department of Defense] installations. A SMEO does not have full DSN [Defense Switched Network] Network Traffic Management capabilities. It offers limited performance reporting and may not support SS7 [Signaling System No. 7] signaling. Therefore, SMEOs will not serve installations that are critical to combatant command missions where NM [network management] control and network visibility for situational awareness is required." [CJCSI 6215.01C]

Softphone An end-user software application on an approved operating system that enables a general-purpose computer to function as a telephony end instrument. It will be tested on an approved operating system as part of the system under test. The Softphone application is considered an IP End Instrument and is associated with the IP telephone switch.

Softswitch A programmable network appliance that:

- Controls connection services for a media gateway and/or native IP end points.
- Selects processes and services that can be applied to a call.
- Provides routing for call control within the network based on signaling and customer database information.

- Transfers control of the call to another network element.
- Interfaces to and supports management functions such as provisioning, fault, and billing.
- Ability to control the access of sessions within and external to its domain. [International Softswitch Consortium]

Strong Authentication The process of authenticating a user based on at least two of three factors: something you know (i.e., username and password), something you have (i.e., token device), and something you are (i.e., fingerprints).

Subscriber The owner of a public key contained in a Public Key Infrastructure certificate. A subscriber may be an appliance or a person.

Survivability The capability of a system to survive in a specified threat environment and accomplish its designated mission.

Synchronization An arrangement for operating digital switching systems at a common (or uniform) clock rate whereby the data signal is accompanied by a phase-related clock. Improperly synchronized clock rates result in the loss of portions of the bit streams and a concomitant loss of information.

System An appliance or group of appliances. The systems described in this document include Multifunction Softswitches, Softswitches, Local Session Controllers, Media Gateways, Border Controllers, End Instruments, LAN switches, and Routers.

System Under Test (SUT) The inclusive components required to test a Unified Capabilities product for Approved Products List certification. Examples of a SUT include Time Division Multiplexing (TDM) or circuit-switch components, Voice over Internet Protocol system components (e.g., Local Session Controller and Gateway), Local Area Network components (e.g., routers and Ethernet switches), and End Instruments.

T

Tactical Network Element (T-NE) A T-NE is any network element used in the tactical network. A T-NE can be used for long local, encapsulated time division multiplexing (TDM), and Proprietary Internet Protocol Trunks.

Tandem Call Trace A feature that identifies the incoming trunk of a tandem call to a specified office directory number. The feature is activated by entering the specified distant office directory number for a tandem call trace. A printout of the incoming trunk number and terminating

directory number, and the time and date is generated for every call to the specified directory number.

Telecom Switch/Device Hardware or software designed to send and receive voice, data, or video signals across a network that provides customer voice, data, or video equipment access to the Defense Switch Network or public switch telecommunications network.

Ten-Digit Dialing The ability to use ten digits comprising the area code, switch code, and line number to establish interswitch calls where the number plan area of the calling party is different from the number plan area of the called party

Terminating Internet Protocol (IP)/Time Division Multiplexing (TDM) Signaling Gateway Function The function related to receiving an Assured Service Session Initiation Protocol (AS-SIP) INVITE from the IP network and sending an Initial Address Message (IAM) onto the Signaling System No. 7 (SS7) network. If the AS-SIP INVITE included an encapsulated Integrated Services Digital Network (ISDN) User Part (ISUP) IAM, then it is decapsulated – identical to Incoming Interworking Unit in International Telecommunications Union – Telecommunication Standardization Sector (ITU-T) Recommendation Q.1912.5, Interworking between Session Initiation Protocol and Bearer Independent Call Control Protocol or ISUP.

Terminating Gateway Assured Service Session Initiation Protocol (AS-SIP) for Telephones signaling appliance performing the terminating Internet Protocol (IP)/Time Division Multiplexing (TDM) Signaling Gateway function in the case of TDM bridging call flows and IP-to-TDM call flows, and either directly serving the destination IP End Instruments or the AS-SIP signaling appliances representing the destination IP End Instruments in the case of TDM-to-IP call flows.

Three-Way Calling A feature that allows a station in the talking state to add a third party to the call without operator assistance.

Throughput The number of octets is successfully transmitted (Internet Protocol) during the measurement interval (typically seconds). Assumes the packets sent do not exceed capacity of the link. [~~NCIDv3 QoS (T300)~~]GESP]

Tracing of Terminating Calls A feature that identifies the calling number on intraoffice calls or the incoming trunk on incoming calls for calls terminating to a specified directory number. When this feature is activated, a printout of the originating directory number or incoming trunk number, terminating directory number, and the time and date is generated for every call to the specified line.

Trace Call in Progress A feature that identifies the originating directory number or incoming trunk for a call in progress. The feature is activated by authorized personnel entering a request that includes the specific terminating directory number or trunk involved in the call.

Traffic Classification A mechanism that allows the networks to distinguish among different categories of traffic, connection requests, and provisioning requests. The classification may be performed at the Edge and Core nodes during packet transport, as well as through indications in the control and management planes for setting up connections and provisioning. Classification can be based on fields in the packets and/or indications in control and management messages.

Traffic Conditioner An entity that performs traffic conditioning functions and may contain meters, markers, droppers, and shapers. Traffic conditioners are typically deployed in Differentiated Services boundary nodes only. A traffic conditioner may re-mark a traffic stream or may discard or shape packets to alter the temporal characteristics of the stream and bring it into compliance with a traffic profile. [RFC 2475]

Traffic Conditioning Control functions performed to enforce traffic classification rules and may include traffic metering, marking, shaping, and policing. Traffic conditioning, when used, will be tied to the parameters chosen for the offered load control.

Traffic Conditioning Agreement (TCA) An agreement specifying classifier rules and any corresponding traffic profiles and metering, marking, discarding, and/or shaping rules that are to apply to the traffic streams selected by the classifier. A TCA encompasses all traffic conditioning rules explicitly specified within a service level agreement along with all the rules implicit from the relevant service requirements and/or from a Differentiated Services domain's service provisioning policy. [RFC 2475]

Traffic Engineering An operator or automaton with the express purpose of minimizing congestion in a network. It encompasses the application of technology and scientific principles to the measurement, modeling, characterization, and control of Internet traffic, and the application of such knowledge and techniques to achieve specific performance objectives. [RFC 2702]

Trunks Time Division Multiplexing (TDM) links used by a circuit switch system to connect to or interconnect Defense Switched Network switches.

Trust Point Public keys (or certificates containing them) that the relying party designates as reliable and trustworthy. The relying party should obtain the public keys (or certificates) through a reliable out-of-band method. Trust points are usually Root Certificates. Under certain circumstances, a relying party may decide to trust an intermediate Certificate Authority (CA) or even an end-entity. Trust is transitive. If the relying party trusts a CA, it also trusts other CAs to which the CA delegates its CA responsibilities. This is also known as a trust anchor.

U

Unified Capabilities (UC) The seamless integration of voice, video, and data services delivered ubiquitously across a secure and highly available network independent of technology infrastructure to provide increased mission effectiveness to the warfighter and business communities. Unified capabilities integrate standards-based communication and collaboration services including, but not limited to, the following:

- Messaging
- Voice, video, and web conferencing
- Unified communication and collaboration applications or clients

These standards-based UC services are integrated with available enterprise applications, both business and warfighting.

User Agent Client (UAC) "A user agent client is a logical entity that creates a new request, and then uses the client transaction state machinery to send it. The role of UAC lasts only for the duration of that transaction. In other words, if a piece of software initiates a request, it acts as a UAC for the duration of that transaction. If it receives a request later, it assumes the role of a user agent server for the processing of that transaction." [RFC 3261]

User Agent Server (UAS) "A user agent server is a logical entity that generates a response to a SIP request. The response accepts, rejects, or redirects the request. This role lasts only for the duration of that transaction. In other words, if a piece of software responds to a request, it acts as a UAS for the duration of that transaction. If it generates a request later, it assumes the role of a user agent client for the processing of that transaction." [RFC 3261]

User Roles Common privileges assigned to users or appliances based on need. The following user roles are defined within the ~~Real Time Services (RTS)~~Unified Capabilities Information Assurance architecture:

- System Security Administrator
  - Defines and assigns user privileges.
  - Adds and deletes user identifications (IDs).
  - Disables or enables the use of specific user IDs as login IDs.
  - Initializes and resets login passwords.
  - Initializes and changes cryptographic keys.
  - Sets the system password aging thresholds.
  - Sets the system limit on the number of failed login attempts.
  - Removes a lockout or changes the system lockout timer value.
  - Sets the system's inactivity timer value.

- Sets system security logging and alarm configuration.
- Manages the system security logging processes.
- Upgrades security software.
- Terminates any user of system session.

- System Administrator

  - Installs appliance.
  - Defines and assigns new user and group privileges at the operating system level.
  - Maintains a record of all requests for login IDs.
  - Adds and deletes users at the operating system level.
  - Disables the use of specific IDs as login IDs (e.g., bin, sys, etc.).
  - Installs operating system updates and patches.
  - Monitors system logs.
  - Maintains and monitors access and changes to SUPERUSER password.
  - Controls access to SUPERUSER account.
  - Manages system logging processes.
  - Delegates administration authorizations to specific persons in other roles.
  - Terminates any user or system session.

- Application Administrator

  - A role responsible for the proper activation, maintenance, and usage of an application on an appliance. Application administrator tasks include upgrading application software.

- Privileged Application User

  - A user with the capability to originate ROUTINE and above ROUTINE precedence ~~RTS~~ sessions

- Application User

  - A user who may execute applications on a system or may originate ROUTINE precedence sessions

V

Video Teleconferencing (VTC) Two-way electronic form of communications that permits two or more people in different locations to engage in face-to-face audio and visual communication.

Meetings, seminars, and conferences are conducted as if all the participants are in the same room.

Video Teleconferencing Unit (VTU) Video teleconferencing end point equipment that performs the following functions: coding/decoding of audio and video; multiplexing of video, audio, data, and control signals; system control; and end-to-end signaling. It may include input/output functions, embedded cryptographic functions, network interface functions, end-to-network signaling, and connections to networks.

Virtual Network Element (VT-NE) A VT-NE is any network element integrated into a certified Defense Switched Network switch. A T-NE can be used for long local, encapsulated time division multiplexing (TDM), and Proprietary Internet Protocol Trunks.

Voice over IP (VoIP) System A set of components required to provide Defense Switched Network (DSN) Internet Protocol (IP) voice services from end instrument to DSN trunk, or IP phone to IP phone. The VoIP system includes, but is not limited to, the IP telephony instrument, the local area network, the Local Session Controller, and the IP gateway.

Voice over Secure Internet Protocol (VoSIP) The instantiation of Internet Protocol (IP) Telephony on a classified local area network or wide area network infrastructure that provides the routing of voice conversations using Secure Internet Protocol Router Network (SIPRNet) as the transport medium. The use of SIPRNet allows users in secure environments to communicate at the Secret level without the need for specialized phones or the use of key material. Bidirectional interoperability with the Defense Red Switch Network is provided through the Defense Information Systems Agency-managed IP-to-Time Division Multiplexing (TDM) interfaces.

Voiceband Data (VBD) (Modem Pass-Through) A subset of Modem over Internet Protocol (IP) in which modem signals are transmitted over the voice channel of a packet network.

W

Wide Area Network (WAN) Level Assured Services Admission Control (W-ASAC) The processes on a Multifunction Softswitch or Assured Real Time Services Softswitch that ensure that quality of service requirements of a higher precedence service will be met at the expense of a lower precedence service if the WAN conditions do not allow meeting quality of service requirements of all services. The processes are typically associated with the preemption of lower precedence sessions within the WAN to ensure that higher precedence sessions can be completed. In addition, the W-ASAC ensures that its subtended Local Session Controllers remain within their traffic engineered real time service allocations.

Wide Area Network Softswitch (WAN SS) A standalone Approved Products List product that acts as an Assured Services Session Initiation Protocol Back-to-Back User Agent within the Unified Capabilities (UC) architecture. It provides the equivalent functionality of a commercial SS and has similar functionality to the SS component of a Multifunction Softswitch (MFSS). The functionality of the Local Session Controller (LSC) is a conditional requirement and the support of a Signaling Gateway is not required. The inclusion of the product in the UC architecture allows the functionality of an MFSS to be achieved by interconnecting two separate appliances (Multifunction Switch and WAN SS), possibly provided by different vendors. The creation of a WAN SS provides Government flexibility in the rollout of UC Voice and Video over Internet Protocol capabilities and eases the migration of time-division multiplexing (TDM) technology based services to IP technology-based services.

Wireless Can refer to either 802.x devices or cellular telephones (see UCR 2010, Section 5.3.1.6.2, Operational Changes, for more details).

Wireless Device An 802.x device or cellular phone.

Wireless Access Bridge (WAB) A device that connects two local area network segments together via wireless transmission.

Wireless End Instrument (WEI) A Defense Switched Network command and control (C2) or non-C2 user device that receives voice service via an IP telephone instrument using wireless technologies, such as 802.11 or 802.16. Also known as a wireless telephony subscriber.

Wireless Local Area Network (LAN) (WLAN) Generic term used to describe the use of wireless technologies in the LAN. The WLAN includes all the wireless terminology (i.e., wireless access bridge, wireless end instrument, and Wireless LAN Access System).

Wireless Local Area Network (LAN) Access System (WLAS) An implementation of wireless technologies considered to be the replacement of the physical layer of the wired Access Layer of a LAN.

SECTION A3
ACRONYMS AND ABBREVIATIONS

~~1R~~	~~Reamplification~~
~~2R~~	~~Reamplification and Reshaping~~
~~2W~~	~~2-Wire~~
3GPP	Third Generation Partnership Project
~~3R~~	~~Reamplification, Reshaping, and Retiming~~
3GSM	Third Global System for Mobile
~~4W~~	~~4-Wire~~
24/7	24-Hours, 7 Days A Week
~~A/D~~	~~Analog/Digital~~
AAF	Army Air Field
AAG	Access Aggregation Function
AAL5	ATM Adaptation Layer 5
~~AAR~~	~~Automatic Alternate Routing~~
~~ABBT~~	~~Automatic Board-to-Board Testing~~
ac	Alternating Current
~~AC~~	~~Admission Control~~
~~ACA~~	~~Automatic Circuit Assurance~~
~~ACAT~~	~~Acquisition Category~~
ACC	Automatic Congestion Control
ACD	Attendant/Call Director
ACD	Automatic Call Distribution
ACD	Automatic Call Distributor
~~ACG~~	~~Automatic Call Gap~~
ACL	Access Control List
ACM	Address Complete Message
~~ACMOS~~	~~Automatic Customer Measurement Outputting System~~
~~ACR~~	~~Anonymous Call Rejection~~
ACTA	Administrative Council for Terminal Attachments
ADIMSS	Advanced DSN Integrated Management Support System
ADM	Add-Drop Multiplexing
ADN	Area Distribution Node
~~ADSI~~	~~Analog Display Services Interface~~
AEI	AS-SIP End Instrument
AES	Advanced Encryption Standard
AF	Assured Forwarding
AF3	Assured Forwarding-3
AF4	Assured Forwarding-4

AFB	Air Force Base
~~AFR~~	~~Automatic Flexible Routing~~
~~AFSCN~~	~~Air Force Satellite Control Network~~
AG	Access Gateway
AGF	Access Grooming Function
AHWG	Ad Hoc Working Group
~~AIN~~	~~Advanced Intelligent Network~~
~~AIOD~~	~~Automatic Identified Outward Dialing~~
AIS	Alarm Indication Signal
AIS	Automated Information System
AIS-CI	Alarm Indication Signal – Customer Installation
~~ALI~~	~~Automatic Location Identification~~
A-link	Access Link
~~ALIT~~	~~Automatic Line Insulation Test~~
AMA	Automatic Message Accounting
AMI	Alternate Mark Inversion
AMR	Adaptive Multi-Rate
AMSL	Above Mean Sea Level
~~AN/TTC-39~~	~~Army Navy/Transportable Telephone Communications~~
~~ANAT~~	~~Alternative Network Address Types~~
AND	Area Distribution Node
~~ANDVT~~	~~Advanced Narrowband Digital Voice Terminal~~
~~ANI~~	~~Automatic Number Identification~~
ANM	Answer Message
ANS	Answer Message
ANSI	American National Standards Institute
AOR	Address of Record
AOR	Area of Responsibility
APL	Approved Products List
APRI	Address Presentation Restricted Indicator
APS	Automatic Protection Switching
~~AR~~	~~Access Router~~
AR	Aggregated Router
AR	Aggregation Router
~~AR~~	~~Automatic Recall~~
ARD	Automated Receiving Device
ARP	Address Resolution Protocol
~~ARS~~	~~Automatic Route Selection~~
~~ARTS~~	~~Assured Real Time Services~~
AS	Assured Services
AS	Application-Specific Maximum
AS	Autonomous System

ASAC	Assured Services Admission Control
ASCII	American Standard Code for Information Interchange
ASD(NII)	Assistant Secretary of Defense for Networks & Information Integration
ASF	Assured Services Features
ASLAN	Assured Service Local Area Network
~~ASP~~	~~Application Server Process~~
AS-SIP	Assured Services Session Initiation Protocol
AS-SIP-T	Assured Services Session Initiation Protocol for Telephones
~~AT~~	~~Access Tandem~~
ATA	Analog Terminal Adapter
ATC	Authority to Connect
ATIS	Alliance for Telecommunications Industry Solution
ATM	Asynchronous Transfer Mode
ATO	Authority to Operate
ATP	Acceptance Test Procedure/Plan
ATQA	Attendant Queue Announcement
AU-3	Administrative Unit-3
AU-4	Administrative Unit-4
AU-4-Xc	Administrative Unit-4-Xc
AUC	Authentication Center
Auth	Authorization
~~AVC~~	~~Advanced Video Coding~~
AVP	Audio/Video Profile
AVPF	Audio-Visual Profile with Feedback
B/P/C/S	Base/Post/Camp/Station
B2BUA	Back-to-Back User Agent
B3ZS	Bipolar 3 Zero Substitution
B8ZS	Bipolar with Eight-Zero Substitution
BA	Billing Agent
BAF	Bellcore AMA Format
BASE	Baseband
BB	Backbone
~~BBG~~	~~Basic Business Group~~
BC	Bearer Capability
BC	Border Controller
~~BCC~~	~~Bellcore Client Company~~
~~BCE~~	~~Bridged Call Exclusion~~
BCI	Backwards Call Indicator
~~BCLID~~	~~Bulk Calling Line Identification~~
~~BCP~~	~~Best Current Practice~~

BE	Block Error
BE	Best Effort
BEHAVE	Behavior Engineering for Hindrance Avoidance
BER	Bit Error Rate
BERT	Bit Error Rate Tester
BFCP	Binary Floor Control Protocol
~~BG~~	~~Business Group~~
~~BGAC~~	~~Business Group Automatic Callback~~
~~BGCW~~	~~Business Group Call Waiting~~
~~BGL~~	~~Business Group Line~~
BGMP	Border Gateway Multicast Protocol
BGP	Border Gateway Protocol
BGP-4	Border Gateway Protocol 4
BICC	Bearer-Independent Call Control
~~BIP-N~~	~~Bit Interleaved Parity-Number~~
BITS	Building Integrated Timing Supply
BLSR	Bidirectional Line Switched Ring
BLV	Busy Line Verification
BNEA	Busy Not Equipped Announcement
BNF	Backus-Naur Form
BOOTP	Bootstrap Protocol
BPV	Bipolar Violation
BPA	Blocked Precedence Announcement
BPP	BitsPerPictureMaxKb
bps	Bits per Second
~~BRA~~	~~Basic Rate Access~~
BRAC	Base Realignment and Closure
BRI	Basic Rate Interface
BSC	Base Station Controller
BSR	Bootstrap Router
BSS	Base Station Subsystem
BTS	Base Transceiver Station
BW	Bandwidth
C	Conditional
C&A	Certification and Accreditation
C/P/S	Camp, Post, or Station
C2	Command and Control
~~C2(R)~~	~~C2 User (Originate ROUTINE Only Calls)~~
~~C2I~~	~~Command, Control, and Intelligence~~
C4	Command, Control, Communications, and Computers
~~C4I~~	~~Command, Control, Communications, Computers, and Intelligence~~

~~C4ISP~~	~~C4 Information Support Plan~~
CA	Certificate/Certification Authority
CAA	Certification Approval Authority
CAC	Call Admission Control
CAC	Common Access Card
~~CAD~~	~~Computer-Assisted Dispatch~~
CAG	Channel Access Grooming
CAL	Confidential Access Level
CALEA	Communications Assistance to Law Enforcement Act
~~CAMA~~	~~Centralized Automatic Message Accounting~~
CAN	Campus Area Network
CANF	Cancel From
CANT	Cancel To
~~CAP~~	~~Competitive Access Provider~~
~~CAROT~~	~~Centralized Automatic Reporting On Trunks~~
CAS	Channel-Associated Signaling
~~CAT~~	~~Customer Access Treatment~~
CAT	Category
CAT5	Category 5
~~CBCS~~	~~Common Baseline Circuit Switch~~
CB-WFQ	Class-Based~~s~~ WFQ
CC/S/A	Combatant Commander/Service/Agency
CCA	Call Connection Agent
CCA	Call Control Agent
CCAT	Continuous Concatenation
CCB	Configuration Control Board
~~CCC~~	~~Clear Channel Capability~~
~~CCEP~~	~~Commercial COMSEC Evaluation Program~~
~~CCI~~	~~Controlled Cryptographic Item~~
CCITT	International Telegraph and Telephone Consultative Committee (now ITU-T)
CCM	Codex Control Message
CCM	Configuration Control and Management
CCMP	Counter with Cipher Block Chaining-Message Authentication Code Protocol
~~ccs~~	~~Hundred Call Seconds~~
CCS	Common Channel Signaling
CCS7	Common Channel Signaling System No. 7
~~CCSA~~	~~Common Control Switching Arrangement~~
~~CCSN~~	~~Common Channel Signaling Network~~
~~CDAR~~	~~Customer-Dialed Account Recording~~
~~CDIMP~~	~~Combined Information Management Panel~~

~~CDMA~~	~~Code Division Multiple Access~~
~~CDMA2000~~	~~Code Division Multiple Access 2000~~
~~CdPA~~	~~Called Party Address~~
CDR	Call Detail Recording
CDR	Call Detail Record
~~CDR~~	~~Critical Design Review~~
CE	Customer Edge
CE Router	Customer Edge Router
~~CEPT~~	~~Commission of European Post and Telecommunication~~
CES	Circuit Emulation Service
~~CESoP~~	~~Circuit Emulation Service over Packet~~
~~CEU~~	~~Channel Encryption Unit~~
CF	Call Forwarding
CFB	Call Forwarding Busy
CFBL	Call Forwarding Busy Line
CFDA	Call Forwarding - Don't Answer
CFI	Canonical Format Indicator
CFR	Code of Federal Regulations
CFV	Call Forwarding Variable
CGA	Carrier Group Alarm
~~CGAP~~	~~Call Gapping~~
CGB	Circuit Group Blocking Message
CgPA	Calling Party Address
CgPN	Calling Party Number
~~CHBK~~	~~Channel Bank~~
CI	Customer Installation
~~CIA~~	~~Central Intelligence Agency~~
CIC	Circuit Identification Code
~~CID~~	~~Calling Identity Delivery~~
CID	Craft Input Device
~~CID~~	~~Craft Interface Device~~
~~CIDCW~~	~~Calling Identity on Call Waiting~~
~~CIDR~~	~~Classless Inter-Domain Routing~~
~~CIDS~~	~~Calling Identity Delivery and Suppression~~
CIO	Chief Information Officer
~~CIR~~	~~Committed Information Rate~~
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CJCSM	Chairman of the Joint Chiefs of Staff Manual
Ckt	Circuit
~~CLAN~~	~~Converged Local Area Network~~
CLI	Calling Line Identification

~~CLID~~	~~Calling Line Identifier~~
CM	Configuration Management
CM	Countermeasure
CM	Cryptographic Modernization
~~CMC~~	~~Cellular Mobile Carrier~~
CMI	Cryptographic Modernization Initiative
~~CN~~	~~Core Network~~
~~CNAB~~	~~Calling Name Delivery Blocking~~
~~CNAM~~	~~Calling Name Delivery~~
~~CND~~	~~Calling Number Delivery~~
~~CND~~	~~Computer Network Defense~~
~~CNDB~~	~~Calling Number Delivery Blocking~~
CNT	Count
CO	Central Office
~~COA~~	~~Changeover Acknowledgement~~
COCOM	Combatant Commander
codec	Coder/Decoder
COI	Community of Interest
COIN	Community of Interest Network
COMSEC	Communications Security
CON	Connect
CONOPS	Concept of Operations
CONUS	Continental United States
~~COO~~	~~Changeover Order~~
~~COP WAT~~	~~Customer-Owned Premises Wiring Acceptance Test~~
COPS	Common Open Policy Service
CoS	Class of Service
COS	Class of Service
COT	Continuity Testing
COT	Customer Originated Trace
COTS	Commercial Off-the-Shelf
CPC	Calling Party Category
C-PE	Classified Provider Edge
CPE	Customer Premises Equipment
CPCF	Custom Picture Clock Frequency
CPG	Call Progress Message
~~CPS~~	~~Customer Premises System~~
CPSG	Call Park Subscriber Group
CPT	Cryptographic Products Testing
~~CPTE~~	~~Customer Premises Terminal Equipment~~
CPU	Central Processing Unit
CQ	Custom Queuing

CR	Customer Router
CRC	Cyclic Redundancy Check
CRD	~~Capstone~~ Capabilities Requirements Document
~~Crypto~~	~~Cryptographic~~
~~CS~~	~~Call Screening~~
CS	Circuit-Switched
CS	Class Selector
~~CS~~	~~Content Staging~~
~~CS/IDM~~	~~Content Staging/Information Dissemination Management~~
~~CS-ACELP~~	~~Conjugate-Structure Algebraic-Code-Excited Linear Prediction~~
CSeq	Command Sequence
~~CSN~~	~~Canadian Switched Network~~
CSPF	Constrained Shortest Path First
~~CSR~~	~~Customer Station Rearrangement~~
CSU	Channel Service Unit
~~CT~~	~~Call Trace~~
CTI	Computer Telephony Integration
CTL	Certificate Trust List
CUG	Closed User Group
CV	Cod~~e~~ing Violation~~s~~
CVSD	Continuously Variable Slope Delta
CVVoIP	Classified Voice and Video over IP
CW	Call Waiting
~~CWD~~	~~Call Waiting Deluxe~~
~~CWI~~	~~Call Waiting Indication~~
~~CWT~~	~~Call Waiting Terminating~~
CY	Calendar Year
~~D/A~~	~~Digital/Analog~~
~~D3~~	~~Third Generation Channel Bank~~
~~D4~~	~~Fourth Generation Channel Bank~~
~~D5~~	~~Fifth Generation Channel Bank~~
DA	Destination Address
~~DA~~	~~Directory Assistance~~
DAA	Designated Accrediting/Approval Authority
DAC	Discretionary Access Control
DAD	Duplicate Address Detection
DAM	Diagnostic Acceptability Measure
~~DARTS~~	~~DISN Assured Real Time Services~~
~~dB~~	~~Decibel~~
DBMS	Database Management System
dc	Direct Current

DCC	Data Communications Channel
DCE	Data Communication Equipment
~~DCIO~~	~~Deputy Chief Information Officer~~
DCN	Data Communications Network
~~DCP~~	~~Designated Called Party~~
~~DCTN~~	~~Defense Commercial Telecommunications Network~~
DCVX	Deployed Cellular Voice Exchange
D-D	Deployable-to-Deployable
~~DDD~~	~~Direct Distance Dialing~~
DEMUX	Demultiplexer
~~DES~~	~~Data Encryption Standard~~
DF	Default
~~DFSU~~	~~Dual Frequency Signaling Unit~~
DHCP	Dynamic Host Configuration Protocol
DIA	Defense Intelligence Agency
DIACAP	Defense Information Assurance Certification and Accreditation Process
~~DICE~~	~~DoD Interoperability Communications Exercise~~
~~DID~~	~~Direct Inward Dialing~~
DiffServ	Differentiated Services
DISA	Defense Information Systems Agency
~~DISAC~~	~~Defense Information Systems Agency Circular~~
DISN	Defense Information System Network
DISR	DoD Information Technology Standards Registry
~~DITSCAP~~	~~DoD Information Technology Security Certification and Accreditation Process~~
~~DIU~~	~~Digital Interface Unit~~
DLC	Digital Loop Carrier
DLoS	Direct Line of Sight
DLSC	Deployed Local Session Controller
DMS	Defense Message System
DMSC	Deployed Mobile Switching Center
DEMUX	Demultiplexer
DMZ	Demilitarized Zone
DN	Directory Number
D-NE	Deployed Network Element
DNS	Domain Name System
~~DOC~~	~~Dynamic Overload Control~~
DoD	Department of Defense
~~DOD~~	~~Direct Outward Dialing~~
DODAF	Department of Defense Architecture Framework
DoDD	DoD Directive

DoDI	DoD Instruction
DoS	Denial of Service
DOTS	"DISN Overarching Technical Strategy"
~~DP~~	~~Dial Pulse~~
DPC	Destination Point Code
~~DRCW~~	~~Distinctive Ringing/Call Waiting~~
~~DRE~~	~~Directional Reservation Equipment~~
DRSN	Defense Red Switch Network
DRT	Diagnostic Rhyme Test
~~DS~~	~~Data Set~~
DS	Differentiated Services
DS	Digital Signal
DS0	Digital Signal Level 0
DS1	Digital Signal Level 1
DS3	Digital Signal Level 3
DS12	Digital Signal Level 12
DSAWG	DISN Security Accreditation Working Group
DSCD	DoD Secure Communications Device
DSCP	Differentiated Services Code Point
DS Field	Differentiated Services Field
DSMCU	Dual-Signaling Multipoint Control Unit
DSN	Defense Switched Network
DSS	DISN Subscription Service
~~DSS1~~	~~Digital Subscriber Signaling System No. 1~~
DSSS	Dual-Signaling Softswitch
DSU	Digital Service Unit
~~DSVT~~	~~Digital Subscriber Voice Terminal~~
~~DTAU~~	~~Digital Test Access Unit~~
DTE	Data Terminal Equipment
DTEP	"DISN Technology Evolution Plan"
~~DTG~~	~~Date Time Group~~
DTMF	Dual-Tone Multifrequency
DTR	Desktop Review
DTU	Digital Test Unit
~~DVMRP~~	~~Distance Vector Multicast Routing Protocol~~
DVS	DISN Video Services
~~DVS-G~~	~~DISN Video Services-Global~~
~~DVS-II~~	~~DISN Video Services II~~
DVX	Deployable Voice Exchange
DVX-C	Deployable Voice Exchange – COTS
DVX-L	Deployable Voice Exchange – Legacy
DWDM	Dense Wave Division Multiplex

E&M	Ear and Mouth
~~E/NM~~	~~Enterprise and Network Management~~
E2E	End-to-End
E911	Enhanced Emergency Service
EA	Enterprise Architecture
~~EA1~~	~~Emergency Announcement 1~~
~~EA2~~	~~Emergency Announcement 2~~
~~EADAS~~	~~Engineering and Administration Data Acquisition System~~
~~EAEO~~	~~Equal Access End Office~~
~~EAOSS~~	~~Exchange Access Operator Services System~~
EAP	Extensible Authentication Protocol
EA-TJTN	Executive Agent for Theater Joint Tactical Networks
EAL4	Evaluated Assurance Level 4
EBC	Edge Boundary Controller
EBER	Excessive Bit Error Rate
eBGP	External Border Control Protocol
EC	Echo Canceller
EC	European Community
ECAR-1	Enclave and Computing Environment Audit Record Content-1
ECAR-2	Enclave and Computing Environment Audit Record Content-2
ECAR-3	Enclave and Computing Environment Audit Record Content-3
ECN	Explicit Congestion Notification
~~ECO~~	~~Embedded Operations Channel~~
ECTP-1	Enclave and Computing Environment Audit Trail Protection-1
ECU	End Cryptographic Unit
EDC	Electronic Dispersion Compensation
~~EDU~~	~~Electronic Dispersion Compensation~~
EF	Expedited Forwarding
~~EF~~	~~Extended Frame~~
EF&I	Engineer, Furnish, and Install
~~EFEC~~	~~Enhanced Forward Error Correction~~
~~EGP~~	~~Exterior Gateway Protocol~~
EI	End Instrument
EIA	Electronics Industries Alliance
EIR	Equipment Identity Register
~~EIS~~	~~Expanded Inband Signaling~~
~~EKTS~~	~~Electronic Key Telephone System~~
E-LSP	EXP-Inferred LSP
~~E-LEAF~~	~~Expanded Large Effective Area Fiber~~
~~eLSR~~	~~Edge Label Switch Router~~
EMC	Electromagnetic Compatibility

EMI	Electromagnetic Interference
eMLPP	Enhanced Multilevel Precedence and Preemption
~~EML~~	~~Electromagnetic Launcher, Levitation, Log(?)~~
EMS	Element Management System
~~EMSS~~	~~Enhanced Mobile Satellite Systems~~
ENUM	Electronic Numbering
EO	End Office
~~EOC~~	~~Embedded Operations Channel~~
EOL	End of Life
~~EOS~~	~~End Office Switch~~
~~EPSCS~~	~~Enhanced Private Switched Communication Service~~
ertPS	Extended Real-Time Polling Service
~~ES~~	~~Enterprise Services~~
ES	Errored Seconds
ESCON	Enterprise Systems Connection
ESD	Electrostatic Discharge
ESF	Extended Superframe
~~ESN~~	~~Extended Sequence Number~~
ESONET	Enhanced Synchronous Optical Network
~~ESOP~~	~~Enhanced Switch Operation Program~~
ESP	Encapsulating Security Payload
ESP	Essential Service Protection
ET	End Terminal
~~ETN~~	~~Electronic Tandem Network~~
ETS	Electronic Tandem Switching
ETSI	European Telecommunications Standards Institute
EUB	End User Building
EV-DO	Evolution-Data Optimized
EVDO	Evolution-Data Optimized
F	Factor
F	FLASH
~~FA~~	~~Forwarding Adjacency~~
FAS	Facility Associated Signaling
Fax	Facsimile
FBI	Federal Bureau of Investigation
~~FC~~	~~Facility Code~~
FCAPS	Fault, Configuration, Accounting, Performance, and Security
FCC	Federal Communications Commission
FCI	Forward Call Indicators
F-D	Fixed-to-Deployable
~~FD~~	~~Feature Definition~~

FDL	Facility Data Link
FDM	Frequency-Division Multiplexing
FDSP	Fiber Service Delivery Point
FE	Fast Ethernet
FEAC	Far-End Alarm and Control
FEBE	Far-End Block Error
~~FEC~~	~~Forward Equivalence Class~~
FEC	Forward Error Correction
FECC	Far-End Camera Control
~~FEMF~~	~~Foreign Electromotive Force~~
FEOOF	Far-End Out of Frame
F-F	Fixed-to-Fixed
FFR	Fast Failure Recovery
~~FGA~~	~~Feature Group A~~
~~FGB~~	~~Feature Group B~~
~~FGC~~	~~Feature Group C~~
~~FGD~~	~~Feature Group D~~
~~FGE~~	~~Feature Group E~~
~~FGF~~	~~Feature Group F~~
FICON	Fiber Connectivity
FIFO	First-In First-Out
FIPS	Federal Information Processing Standard
FIR	Full Intra Request
FISMA	Federal Information Security Management Act
~~FISU~~	~~Fill-In Signaling Unit~~
FNBDT	Future Narrowband Digital Terminal
F-NE	Fixed Network Element
FNPA	Foreign Numbering Plan Area
FO	FLASH OVERRIDE
FOC	Final Operational Capability
FoIP	Facsimile over Internet Protocol
FOO	FLASH OVERRIDE OVERRIDE
FQDN	Fully Qualified Domain Name
~~FR~~	~~Family of Requirements~~
~~FRL~~	~~Facility Restriction Level~~
FRR	Fast Reroute
FSD	Feature Service Description
FSD	Feature Specific Document
FSDP	Fiber Service Delivery Point
FSO	Field Security Office
F-T	Fixed-to-Tactical
ft	Foot

FT	Fast Track
FTR	Federal Telecommunications Recommendation
~~FTS~~	~~Federal Technology Service~~
~~FTS~~	~~Federal Telecommunications Systems~~
~~FTS~~	~~Federal Telephone System~~
FTP	File Transfer Protocol
FW	Firewall
FX	Foreign Exchange
FY	Fiscal Year
G3	Group 3
G3 Fax	Group 3 Facsimile
~~GAO~~	~~Government Accounting Office~~
GbE	Gigabit Ethernet
GBNP	Global Block Numbering Plan
Gbps	Gigabits per Second
GCIRD	Generic Cryptographic Interoperability Requirements Document
~~GCM~~	~~GIG Content Management~~
GE	Gigabit Ethernet
GEI	Generic End Instrument
GEM	GIG Enterprise Management
GESP	GIG Enterprise Service Profile
~~GETS~~	~~Government Emergency Telecommunications System~~
GFP	Generic Framing Procedure
GHz	Gigahertz
GIG	Global Information Grid
GIG 2.0	Global Information Grid 2.0
GIG-BE	Global Information Grid – Bandwidth Expansion
GLS	Global Location Server
GMPLS	Generalized Multiprotocol Label Switching
~~GNA~~	~~GIG Net Assurance~~
~~GNE~~	~~Gateway Network Element~~
GNSC	Global Network Support Center
GOS	Grade of Service
GOTS	Government Off-the-Shelf
GPS	Global Positioning System
GR	Generic Requirement
GRE	Generic Routing Encapsulation
GRS	Circuit Group Reset Message
~~GSA~~	~~General Services Agency~~
~~GSCR~~	~~Generic Switching Center Requirements~~
GSM	Global System for Mobile

GSR	Generic System Requirement
~~GSS~~	~~Generic System Specification~~
GSTP	Generic Switching Test Plan
~~GSVS~~	~~Global Secure Voice System~~
~~GTKPR~~	~~Gatekeeper~~
~~GTT~~	~~Global Title Translation~~
~~GUI~~	~~Graphical User Interface~~
HAIPE	High Assurance Internet Protocol Encryptor
~~HAIPES~~	~~Secure High Assurance Internet Protocol Encryptor~~
~~HDB3~~	~~High Density Bipolar 3 Code~~
HDLC	High-Level Data Link Control
HEMP	High-Altitude Electromagnetic Pulse
HEX	Hexadecimal
HLC	High Layer Compatibility
HLR	Home Location Register
~~HNPA~~	~~Home Numbering Plan Area~~
~~H-R~~	~~Host Remote (Link)~~
hr	Hour
HRD	Hypothetical Reference Decoder
~~HSRP~~	~~Hot Standby Router Protocol~~
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol, Secure
~~HTR~~	~~Hard-To-Reach~~
Hz	Hertz
I	IMMEDIATE
I&A	Identification and Authentication
~~I&S~~	~~Interoperability and Supportability~~
IA	Information Assurance
~~IA/CND~~	~~Information Assurance/Computer Network Defense~~
~~IAA~~	~~Information Assurance Accreditation~~
IAD	Integrated Access Device
IAM	Initial Address Message
IANA	Internet Assigned Numbers Authority
IAO	Information Assurance Officer
IAS	Integrated Access Switch/System
IASRD	Information Assurance Security Requirements Document
IATC	Interim Authority to Connect
IATO	Interim Authority to Operate
IATP	Information Assurance Test Plan
IATT	Information Assurance Test Team

IATT	Interim Authority to Test
IAVA	Information Assurance Vulnerability Alert
IAVM	Information Assurance Vulnerability Management
IAW	In Accordance With
iBGP	Internal Border Control Protocol
~~IBNT2~~	~~Integrated Business Network Trunk Type II (Nortel Trunk Type)~~
~~IC~~	~~Inter-LATA Carrier~~
IC	Interexchange Carrier
ICA	Isolated Code Announcement
ICCS	Intra-Cluster Communication Signaling
ICD	Initial Capabilities Document
ICE	Interactive Connectivity Establishment
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol for IPv6
~~ICTO~~	~~Interim Certification to Operate~~
ID	Identification
~~IDDD~~	~~International Direct Distance Dialing~~
IDLC	Integrated Digital Loop Carrier
~~IDM~~	~~Information Dissemination Management~~
IDNX	Integrated Digital Network Exchange
IDR	Instantaneous Decoder Refresh
IDR	Inter-Domain Routing
~~IDS~~	~~Integrated Data Services~~
IDS	Intrusion Detection System
IDT	Integrated Digital Terminal
Ie	Equipment Impairment Factor
IE	Information Element
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers, Inc.
~~IESG~~	~~Internet Engineering Steering Group~~
IETF	Internet Engineering Task Force
IGMP	Internet Group ~~Multicast~~ Management Protocol
IGMPv3	Internet Group Management Protocol, Version 3
~~IGP~~	~~Interior Gateway Protocol~~
I-IWU	Incoming Interworking Unit
IKE	Internet Key Exchange
IKEv1	Internet Key Exchange Version 1
IKEv2	Internet Key Exchange Version 2
ILMI	Integrated Local Management Interface
IM	Instant Messaging
~~IMASS~~	~~Integrated Multiple Access Switched Service~~
IMUX	Inverse Multiplexer

~~INC~~	~~International Carrier~~
INE	In-Line Network Encryptor
INFOSEC	Information Security
INMS	Integrated Network Management System
Intserv	Integrated Services
~~INWATS~~	~~Inward Wide Area Telecommunications Service~~
I/O	Input/Output
IO	Interoperability
IOC	Initial Operational Capability
IP	Internet Protocol
IPDV	IP Packet Delay Variation
IPLR	IP Packet Loss Ratio
ipm	Impulses Per Minute
IPS	Intrusion Protection System
IPSec	Internet Protocol Security
~~IPSG~~	~~Internet Protocol Signaling Gateway~~
IPT	Integrated Product Team
IPTD	IP Packet Transfer Delay
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IR	Intermediate Reach
~~IRR~~	~~Immediate Reroute~~
~~IRU~~	~~Indefeasible Right of Use~~
IS	Information System
IS	Intermediate System
IS	Interoperability Specification
ISAKMP	Internet Security Association and Key Management Protocol
ISDN	Integrated Services Digital Network
IS-IS	Intermediate System to Intermediate System
ISP	Information Support Plan
IST	Interswitch Trunk
ISUP	ISDN User Part
IT	Information Technology
ITU	International Telecommunications Union
ITU-T	International Telecommunications Union – Telecommunication Standardization Sector
IUA	ISDN User Adaptation
~~IVM~~	~~Internet Voice Mail~~
IVR	Interactive Voice Response
~~IVSN~~	~~Initial Voice Switched Network~~
IWF	Interworking Function
IWU	Interworking Unit

I-x	Intraoffice (Interface)
~~IXC~~	~~Interexchange Carrier~~
JCIDS	Joint Capabilities Integration and Development System
~~JCPAT-E~~	~~Joint C4I Program Assessment Tool-Empowered~~
~~JHITS~~	~~Joint Hawaii Information Transfer System~~
JIC	Joint Interoperability Certification
~~JIDS~~	~~Joint Intrusion Detection System~~
JITC	Joint Interoperability Test Command
~~JMSN~~	~~Joint Military Switched Network~~
JNO	Joint Net-Centric Operations
JNN	Joint Network Node
~~JOIN~~	~~Joint On-Demand Interoperability Network~~
JROC	Joint Requirements Oversight Council
JROCM	Joint Requirements Oversight Council Memorandum
JSCMWG	Joint Services Cryptographic Modernization Working Group
~~JTA~~	~~Joint Technical Architecture~~
JTF	Joint Task Force
JTF-GNO	Joint Task Force – Global Network Operations
~~JTRS~~	~~Joint Tactical Radio System~~
JTTP	Joint Tactics, Techniques, and Procedures
~~JUICE~~	~~Joint User Interoperability Communications Exercise~~
JWICS	Joint Worldwide Intelligence Communications System
kb/s	Kilobits per Second
kbit/s	Kilobits per Second
kbps	Kilobits per Second
KEYMAT	Keying Material
kHz	Kilohertz
Km	Kilometer
KMI	Key Management Infrastructure
~~KPP~~	~~Key Performance Parameter~~
L2	OSI Layer 2
L3	OSI Layer 3
~~LAMA~~	~~Local Automatic Message Accounting~~
LAN	Local Area Network
LATA	Local Access and Transport Area
~~L-ASAC~~	~~LSC Level ASAC~~
~~LASD~~	~~Local Assured Service Domain~~
LBO	Line Buildout
~~LC~~	~~Loop Closure~~

LCAS	Link Capacity Adjustment Scheme
LDAP	Lightweight Directory Access Protocol
LDAPv3	Lightweight Directory Access Protocol, Version 3
LDIF	LDAP Interchange Format
~~LDN~~	~~Local Directory Number~~
LDP	Label Distribution Protocol
~~LDS~~	~~Local Digital Switch~~
~~LEC~~	~~Local Exchange Carrier~~
~~LED~~	~~Light Emitting Diode~~
LEF	Link Encryptor Family
LER	Label Edge Router
~~LFB~~	~~Look-Ahead for Busy~~
~~LFB~~	~~Look Forward Busy~~
~~LIB~~	~~Label Information Base~~
~~LIWA~~	~~Land Information Warfare Activity~~
LLC	Logical Link Control (Sublayer)
LLS	Local Location Server
L-LSP	Label-Only-Inferred LSP
LNP	Local Number Portability
L-n.x	Long-Haul (Interface)
~~LO~~	~~Loop Open~~
LOC	Letter of Compliance
~~LOC~~	~~Lines of Communications~~
LOF	Loss of Frame
LOP	Loss of Pointer
~~LOS~~	~~Loss of Signal~~
~~LOSS~~	~~Loss of Signal Seconds~~
LR	Long Reach
LS	LAN Switch
LSC	Local Session Controller
LSP	Label Switched Path
~~LSP~~	~~Link State PDU~~
~~LSR~~	~~Label Switch Router~~
~~LSR~~	~~Label Switched Router~~
~~LSR~~	~~Label Switching Router~~
LSSGR	LATA Switching Systems Generic Requirements
LSSU	Link Status Signaling Unit
~~LT~~	~~Line Termination Equipment~~
~~LU~~	~~Line Unit~~
~~LUTS~~	~~Locked-Up Trunk Scan~~
m	Meter

M&S	Modeling and Simulation
M13	Multiplexer
M2PA	MTP2 User Peer-to-Peer Adaptation
M2UA	MTP2 User Adaptation
M3UA	MTP3 User Adaptation
MA	Mission Area
MAC	Media Access Control
~~MAC~~	~~Mission Assurance Capability~~
MA ICD	Mission Area Initial Capabilities Document
MAN	Metropolitan Area Network
Mbps	Megabits per Second
~~MCC~~	~~Maintenance Control Center~~
MCEB	Military Communications-Electronics Board
MCN	Main Communication Node
MCS	Mobile Cellular Systems
MCU	Multipoint Conferencing Unit
~~MDII~~	~~Machine-Detected Interoffice Irregularities~~
~~MDR~~	~~Message Detail Recording~~
~~MDR~~	~~Maximum Deployment Range~~
MDT	Mean Downtime
MEGACO	Media Gateway Control
MELPe	Enhanced Mixed Excitation Linear Production
MER	Minimum Essential Requirements
~~MF~~	~~Multifrequency~~
MFS	Multifunction Switch
MFSS	Multifunction Softswitch
MG	Media Gateway
MGC	Media Gateway Controller
MGCP	Media Gateway Control Protocol
MHz	Megahertz
mi	Mile
MIB	Management Information Base
MIB II	Management Information Base II
MIDCOM	Middlebox Communication
MILDEP	Military Department
~~Milstar~~	~~Military Strategic and Tactical Relay System~~
MIME	Multipurpose Internet Mail Extension
~~MIPv6~~	~~Mobile IP Version 6~~
~~MIS~~	~~Management Information System~~
MKI	Master Key Identifier
MLD	Multicast Listener Discovery
MLDv2	Multicast Listener Discovery Version 2

~~MLHG~~	~~Multiline Hunt Group~~
MLPP	Multilevel Precedence and Preemption
MLS	Multilevel Security
~~MLT~~	~~Mechanized Loop Test~~
MMF	Multi-Mode Fiber
~~MOE~~	~~Measure of Effectiveness~~
~~MoIP~~	~~Modem over Internet Protocol~~
MOP	Maintenance Operations Protocol
MOR	Maximum Operational Range
MOS	Mean Opinion Score
~~MOSFP~~	~~Multicast Open Shortest Path First~~
MP	Master Plan
MP-BGP	Multi-Protocol Border Gateway Protocol
~~MPEG~~	~~Motion Picture Experts Group~~
MPI	Minimum Picture Interval
MPLS	Multiprotocol Label Switching
MPLS-TE	Multiprotocol Label Switching – Traffic Engineered
ms	Microsecond
MS	Multiplex Section
~~MSAG~~	~~Master Street Address Guide~~
MSDP	Multicast Source Discovery Protocol
~~MSE~~	~~Mobile Subscriber Equipment~~
msec	Milliseconds
~~MSL-100~~	~~Meridian SL-100~~
MSO	Mobile Switching Office
MSPP	Multi-Service Provisioning Platforms
~~MSR~~	~~Message Storage and Retrieval System~~
MSU	Message Signaling Unit
MTBF	Mean Time between Failures
MTBM	Mean Time between Maintenance
MTIE	Maximum Time Interval Error
MTOSI	Multi-Technology Operations System(s) Interface
MTP	Message Transfer Part
MTP1	Message Transfer Part 1
MTP2	Message Transfer Part 2
MTP3	Message Transfer Part 3
MTR	Maximum Transmission Range
~~MTS~~	~~Message Telephone Service~~
MTTR	Mean Time To Repair
MTU	Maximum Transmission Unit
MU	Message Unit
MUF	Military Unique Features

MUX	Multiplexer
~~MVP~~	~~Multiline Variety Package~~
~~mW~~	~~Milliwatt~~
MWR	Morale, Welfare, and Recreation
N/A	Not Applicable
~~NAC~~	~~Network Administration Center~~
NALU	Network Abstraction Layer Unit
~~NANP~~	~~North American Numbering Plan~~
~~NAP~~	~~Network Access Point~~
~~NAPT~~	~~Network Address Port Translation~~
NAS	Network Access Server
NAT	Network Address Translation
~~NATO~~	~~North Atlantic Treaty Organization~~
~~NAVSTAR~~	~~Navigation Satellite Timing and Ranging~~
~~NC~~	~~Network Cluster~~
~~NCA~~	~~No Circuit Announcement~~
NCES	Net-Centric Enterprise Services
NCI	Network Component Infrastructure
~~NCID~~	~~Net-Centric Implementation Document~~
~~NCIDv2~~	~~Net-Centric Implementation Document Version 2~~
NCM	Network Cluster Member
~~NCO~~	~~Net-Centric Operations~~
NCP	Network Cutover Plan
~~NCS~~	~~National Communications System~~
NCTAMS	Naval Computer and Telecommunications Area Master Station
~~NDAA~~	~~National Defense Authorization Act~~
~~NDC~~	~~Network Data Collection~~
NE	Near End
NE	Network Element
NEBS	Network Equipment-Building System
NEMO	Network Mobility
NetOps	Network Operations
NETOPS	Network Operations
NEXT	Near End Crosstalk
NFAS	Non-Facility Associated Signaling
~~NGO~~	~~Non-Governmental Organization~~
NI	Network Identifier
~~NI~~	~~Network Identity~~
NI-1/2	National ISDN 1/2
NI-1	National ISDN 1
NI-2	National ISDN 2
NIAP	National Information Assurance Partnership

~~NIC~~	~~Network Indicator Code~~
NIC	Network Interface Card
NIPR	Unclassified but Sensitive Internet Protocol
NIPRNet	Unclassified but Sensitive Internet Protocol Router Network
NIPRNET	Unclassified but Sensitive Internet Protocol Router Network
NLAS	No Loss of Active Sessions
~~nm~~	~~Nanometer~~
NM	Network Management
~~NMC~~	~~Network Management Center~~
NMCC	National Military Command Center
NMS	Network Management System
NOA	Nature of Address
NOC	Network Operations Center
~~NORAD~~	~~North American Air Defense~~
NOSC	Network Operations and Security Center
NP	Network Provided
NP	Not Permitted
NP	Number Portability
NPA	Numbering Plan Area
npdi	Number Portability Database Dip Indicator
~~NR~~	~~Not Required~~
NR-KPP	Net-Ready Key Performance Parameter
NRT	Near Real Time
nrtPS	Non-Real-Time Polling Service
ns	Nanosecond
NSA	National Security Agency
~~NSE~~	~~Network Switching Element~~
~~NSLP~~	~~Netware Link Services Protocol~~
~~NS/EP~~	~~National Security Emergency Preparedness~~
NSS	National Security Systems
NT1	Network Termination 1
NT2	Network Termination 2
~~NTI~~	~~Northern Telecom, Inc.~~
NTM	Network Traffic Management
NTMOS	Network Traffic Management Operating System
NTP	Network Time Protocol
~~NUTS~~	~~Non-Usage Trunk Scan~~
O&M	Operations and Maintenance
OA	Optical Amplifier
OADM	Optical Add Drop Multiplexer
OAN	Operational Area Network

OA&M	Operations, Administration, and Maintenance
OC-1	Optical Carrier Level 1
OC-3	Optical Carrier Level 3
OC-3c	Optical Carrier Level 3c
OC-12	Optical Carrier Level 12
OC-12c	Optical Carrier Level 12c
OC-48	Optical Carrier Level 48
OC-48c	Optical Carrier Level 48c
OC-192	Optical Carrier Level 192
OC-192c	Optical Carrier Level 192c
OC-768	Optical Carrier Level 768
OCONUS	Outside the Continental United States
OCN	Original Called Number
~~OCS~~	~~Outgoing Call Screening~~
ODXC	Optical Digital Cross-Connect
O/E	Optical/Electrical
OEO	Optical-to-Electrical-to-Optical
OIF	Optical Internetworking Forum
~~OIM~~	~~Operations Interface Module~~
O-IWU	Outgoing Interworking Unit
OL	Open Loop
OLA	Optical Line Amplifier
~~OMB~~	~~Office of Management and Budget~~
~~ONI~~	~~Operator Number Identification~~
~~OO~~	~~Optical-to-Optical~~
OOB	Out-of-Band
OOBM	Out-of-Band-Management
OOF	Out of Frame
OP	Optical Protection
OPC	Originating Point Code
ORL	Optical Return Loss
~~ORR~~	~~Overflow Reroute~~
OS	Operations System
OSA	Optical Spectrum Analyzer
OSC	On-Line Status Check
~~OSC~~	~~Optical Service Channel~~
OSC	Optical Supervisory Channel
OSD	Office of the Secretary of Defense
OSI	Open Systems Interconnect
OSI	Open Systems Interconnection
OSNR	Optical Signal to Noise Ratio
~~OSP~~	~~Outside Plant~~

OSPF	Open Shortest Path First
OSS	Operational Support System
OTAR	Over-The-Air-Rekey
OTGR	Operations Technology Generic Requirements
~~OTM~~	~~Optical Terminal Multiplexer~~
OTN	Optical Transport Network
~~OTS~~	~~Oahu Telephone System (check)~~
OTS	Optical Transport System
~~OUTWATS~~	~~Outward Wide Area Telecommunications Service~~
p	Probability of Blocking
P	Permitted
P	PRIORITY
P	Provider
~~PAA~~	~~Principal Accrediting Authority~~
~~PABX~~	~~Private Automatic Branch Exchange~~
PAC	Pacific
~~PALA~~	~~Precedence Access Limitation Announcement~~
PAM	Pass Along Message
~~P/AR~~	~~Peak-To-Average Ratio~~
~~PAR~~	~~Pixel Aspect Ratio~~
PAS	Priority Access Service
~~PAT~~	~~Precedence Access Threshold~~
PBAS	Precedence Based Assured Service
PBNM	Policy-Based Network Management
PBX	Private Branch Exchange
PBX1	Private Branch Exchange 1
PBX2	Private Branch Exchange 2
PC	Personal Computer
PC	Point Code
PCD	Precedence Call Diversion
PCM	Pulse Code Modulation
PCMA	Paired Carrier Multiple Access
PCMU	Pulse Code Modulation mu-law
~~PCS~~	~~Personal Communications System~~
PDA	Personal Digital Assistant
~~PDB~~	~~Per-Domain Behavior~~
PDH	Plesiochronous Digital Hierarchy
~~PDMA~~	~~Provisioning-Driven Memory Administration~~
PDU	Protocol Data Unit
PE	Provider Edge
PED	Personal Equipment Device

PEI	Proprietary End Instrument
~~PE-R~~	~~Provider Edge Router~~
PESQ	Perceptual Evaluation of Speech Quality
~~PFAC~~	~~Private Facility Access~~
~~PGS~~	~~Pair Gain System~~
PHB	Per Hop Behavior
PHY	Physical Layer
~~PIC~~	~~Primary Inter-LATA Carrier~~
PII	Personally Identifiable Information
PIM	Protocol Independent Multicast
PIM-SM	Protocol Independent Multicast-Sparse Mode
PIN	Personal Identification Number
~~PING~~	~~Packet Internet Groper~~
PIPT	Proprietary Internet Protocol Trunk
PKE	Public Key Enabled
PKI	Public Key Infrastructure
~~PLAM~~	~~Public Line Activity Monitoring~~
PL/CA	Precedence Level/Calling Area
PLCP	Physical Layer Convergence Protocol
PLL	Phase Locked Loop
PM	Performance Management
PM	Performance Monitoring
~~PM~~	~~Program Manager~~
PMD	Polarization Mode Dispersion
~~PMEF~~	~~Primary Mission Essential Function~~
~~PMO~~	~~Program Management Office~~
PMT	Performance Measurement Tool
PO	Program Office
POM	Program Objective Memorandum
~~POP~~	~~Point of Presence~~
POS	Packet over SONET
POTS	Plain Old Telephone Service
ppm	Parts Per Million
PPP	Point-to-Point Protocol
pps	Pulses per Second
PPS	Packets per Second
~~PPSM~~	~~Ports, Protocols, and Services Management~~
~~PPSN~~	~~Public Packet-Switched Network~~
PQ	Priority Queuing
PRA	Primary Rate Access
~~PRE~~	~~Protectional Reservation Equipment~~
PRI	Primary Rate Interface

ps	Poincaré Sphere
ps/Km$^{1/2}$	PMD Coefficient
PSAP	Public Safety Answering Point (expand in text)
PSDS	Public Switched Digital Service
PSIP	Program and System Information Protocol
PSQM	Perceptual Speech Quality Measure
PSTN	Public Switch Telephone Network
~~PTS~~	~~Public Telecommunications Service~~
~~PTT~~	~~Public Telephone and Telegraph~~
PTT	Push-To-Talk
PV	Proprietary VoIP
PVN	Private Virtual Network
Q	Quality Factor
QoR	Query on Release
QoS	Quality of Service
R	Required
R	Router
R	ROUTINE
RADIUS	Remote Authentication Dial In User Service
~~RAFTN~~	~~Royal Air Force Telephone Net~~
RAI	Remote Alarm Indication
RAI-CI	Remote Alarm Indication - Customer Installation
RAN	Radio Access Network
~~RAO~~	~~Revenue Accounting Office~~
RBF	Radio Bridge Function
~~RC~~	~~Ring Control~~
~~RCD~~	~~Route Control Digit~~
~~RCF~~	~~Remote Call Forwarding~~
~~RCMAC~~	~~Recent Change Memory Administration~~ Center
RDI	Remote Defect Indication
~~RDT~~	~~Remote Digital Terminal~~
REI	Radio End Instrument
REL	Release Message
RES	Resume Message
~~RF~~	~~Radio Frequency~~
RFC	Request for Comment
RFI	Remote Failure Indication
~~RGTR~~	~~Regenerator~~
RIB	Routing Information Base
~~RID~~	~~Router Identification~~

~~RIP~~	~~Routing Management Information~~
~~RIPv1~~	~~Routing Management Information Version 1~~
~~RIPv2~~	~~Routing Management Information Version 2~~
RJ	Registered Jack
RLC	Release Complete Message
RLR	Receive Loudness Rating
~~RLT~~	~~Release Link Trunk~~
RM	Remote Management
RMAS	Remote Memory Administration System
RMON	Remote Monitoring
RMON2	Remote Monitoring 2
RMS	Root Mean Square
ROADM	Reconfigurable Optical Add Drop Multiplexer
~~ROP~~	~~Receive Only Printer~~
~~ROTL~~	~~Remote Office Test Line~~
RP	Rendezvous Point
~~RP~~	~~Request-Priority~~
RPF	Reverse Path Forwarding
RPH	Resource-Priority Header
~~RPOA~~	~~Recognized Private Operating Administration~~
RPR	Resilient Packet Ring
~~RQCR~~	~~Reliability and Quality Generic Requirements~~
~~RQSSGR~~	~~Reliability and Quality Switching Systems Generic Requirements~~
RR	Reroute
~~RSB~~	~~Repair Service Bureau~~
RSC	Reset Circuit Message
~~RSU~~	~~Remote Switching Unit~~
RSVP	Resource Reservation Protocol
RSVP-TE	Resource Reservation Protocol-Traffic Engineering
RTCP	Real Time Control Protocol
RTP	Real Time Protocol
RTP	Release to Pivot
rtPS	Real Time Polling Service
~~RTS~~	~~Real Time Services~~
RTS	Routing and Translation Server
RTT	Round-Trip Time
~~RTU~~	~~Remote Test Unit~~
Rx	Receive
~~S&NM~~	~~Systems and Network Management~~
S&U	Secure and Unsecure
SA	Security Association

~~SA~~	~~Services Agent~~
SA	Situational Awareness
SA	Source Address
~~SA~~	~~Stand-Alone (Switch)~~
~~SAC~~	~~Service Access Code~~
SAC	Session Admission Control
SAD	Security Association Database
SAFI	Sub-Address Family Identifier
SAL	Security Access Level
SAN	Storage Area Network
S-AR	Secret Aggregation Router
SAR	Segmentation and Reassembly
SAS	Standalone Switch
SATCOM	Satellite Communications
SBC	Session Border Controller
SBU	Sensitive, But Unclassified
SC/A	Signal Converter/Allotter
~~SCAMPI~~	~~Standard CMMI Assessment Method for Process Improvement~~
SCCP	Signaling Connection Control Part
SCCP	Signaling Connection Control Protocol
SCCS	Switching Control Center System
S-CE	Secret Customer Edge Router
SCF	Selective Call Forwarding
SCIP	Secure Communications Interoperability Protocol
SCN	Switched Circuit Network
~~SCOF~~	~~Selective Control of Facilities~~
SCP	Service Control Point
~~SCR~~	~~Selective Call Rejection~~
SCS	Session Control and Signaling
~~SCSF~~	~~Session Control and Signaling Function~~
SCTP	Stream Control Transmission Protocol
SD	Signal Degrade
~~SDES~~	~~Session Descriptions~~
SDH	Synchronous Digital Hierarchy
SDN	Service Delivery Node
SDP	Session Description Protocol
SDTI	SONET Digital Trunk Interface
SEF	Severely Errored Frame
SEF	Severely Errored Framing
SEFS	Severely Errored Framing Seconds
SEI	Secure End Instrument
SEP	Signaling End Point

~~SES~~	~~Service Evaluation System~~
~~SES~~	~~Severely Errored Seconds~~
~~SF~~	~~Signal Fail~~
SF	Superframe
SFD	Start Frame Delimiter
~~SFG~~	~~Simulated Facilities Group~~
SG	Signaling Gateway
SI	Service Indicator
~~SIB~~	~~Status Indication Busy~~
SIGTRAN	Signaling Transport
SILC	Selective Incoming Load Control
SIMPLE	SIP for Instant Messaging and Presence Leveraging Extensions
SIO	Status Indication Out-of Alignment
SIP	Session Initiation Protocol
SIPO	Signal Units Indicating Processor Outage
SIPR	Secure Internet Protocol Router
SIPRNet	Secure Internet Protocol Router Network (check which is correct)
SIPRNET	Secure Internet Protocol Router Network
SIPS	Session Initiation Protocol Secure
SIP-T	Session Initiation Protocol for Telephones
SIP-T(AS)	SIP-T (Assured Service)
SIPv2	Session Initiation Protocol, Version 2
SIT	Special Information Tone
SLA	Service Level Agreement
SLAAC	Stateless Address Auto-Configuration
~~SLC~~	~~Service Level Commitment~~
SLC	Signaling Link Code
SLR	Send Loudness Rating
~~SLS~~	~~Service Level Specification~~
SLS	Signaling Link Selection
~~SLT~~	~~Signaling Link Test~~
SLTE	Signaling Link Terminal Equipment
~~SLU~~	~~Subscriber Line Usage~~
SMC	SONET Minimum Clock
~~SMDF~~	~~Subscriber Main Distributing Frame~~
~~SMDI~~	~~Simplified Message Desk Interface~~
~~SMDR~~	~~Station Message Detail Recording~~
SME	Subject Matter Expert
SME PED	Secure Mobile Environment Portable Electronic Device
SMEO	Small End Office
SMF	Single Mode Fiber
SMI	Security Management Infrastructure

SMIv2	Structure of Management Information Version 2
SMTP	Simple Message Transfer Protocol (needs expanded in text)
~~SMU~~	~~Switch Multiplex Unit~~
~~SMU~~	~~Switch Multiplexing Unit~~
SNAP	System/Network Approval Process
SNCP	Subnetwork Connection Protection
S-NE	Strategic Network Element
SNMP	Simple Network Management Protocol
SNMPv1	Simple Network Management Protocol, Version 1
SNMPv2	Simple Network Management Protocol, Version 2
SNMPv3	Simple Network Management Protocol Version 3
SNR	Signal to Noise Ratio
S-n.x	Short-Haul (Interface)
~~SOC~~	~~Service Observing Circuit~~
SONET	Synchronous Optical Network
SPC	Signaling Point Code
SPCS	Stored Program Control System (needs expanded in text)
SPD	Security Policy Database
S-PE	Secret Provider Edge
SPF	Shortest Path First
SPFI	Substandard Performance Fault Isolation
SPI	Security Parameter Index
~~SPID~~	~~Service Provider Identifier~~
SpoA	Service Point of Attachment
~~SPRING~~	~~Shared Protection Ring~~
~~SPRM~~	~~Supplemental Performance Report Message~~
SQF	System Quality Factors
SQL	Structured Query Language
SR	Selective Router
SR	Short Reach
SRTCP	Secure Real-Time Transport Control Protocol
SRTP	Secure Real-Time Transport Protocol
SS	Softswitch
SS7	Signaling System No. 7
SSA	Subsystem-Allowed
SSAA	System Security Authorization Agreement
SSH	Secure Shell
SSHv2	Secure Shell Version 2
SSL	Secure Socket Layer
SSM	Single System Manager
SSM	Source-Specific Multicast
SSM	Synchronization Status Message

~~SSMF~~	~~Standard Single Mode Fiber~~
~~SSN~~	~~Subsystem Number~~
~~SSP~~	~~Service Switching Point~~
SSP	Subsystem-Prohibited
~~SSS~~	~~Single Shelter Switch~~
SST	Subsystem Status Test
ST	Signaling Terminal
~~STANAG~~	~~Standard NATO Agreement~~
STE	Secure Terminal Equipment
STEP	Standardized Tactical Entry Point
STIG	Security Technical Implementation Guide
STM	Synchronous Transport Module
STM-1	Synchronous Transport Module 1
STM-1c	Synchronous Transport Module 1c
STM-4	Synchronous Transport Module 4
STM-4c	Synchronous Transport Module 4c
STM-16	Synchronous Transport Module 16
STM-16c	Synchronous Transport Module 16c
STM-64	Synchronous Transport Module 64
STM-256	Synchronous Transport Module 256
STM-O	Synchronous Transport Module O
~~STO~~	~~Special Technical Operations~~
~~STP~~	~~Serial to IP~~
STP	Signaling Transfer Point
STRATCOM	United States Strategic Command
STS	Synchronous Transport Signal
STS-1	Synchronous Transport Signal-1
~~STS-3c~~	~~Synchronous Transport Signal-3c~~
~~STS-12c~~	~~Synchronous Transport Signal-12c~~
~~STS-48~~	~~Synchronous Transport Signal-48~~
~~STS-192c~~	~~Synchronous Transport Signal-192c~~
~~STS-768c~~	~~Synchronous Transport Signal-768c~~
STU	Secure Telephone Unit
~~STU~~	~~Secure Terminal Unit~~
~~STU-II~~	~~Secure Telephone Unit, Second Generation~~
STU-III	Secure Telephone Unit, Third Generation
STU-III/R	Secure Telephone Unit, Third Generation (needs expanded in text)
STUN	Simple Tunneling of UDP through NAT
SU	Signal Unit
SUA	SCCP User Adaptation
~~super-FEC~~	~~Super Forward Error Correction~~
SUS	Suspend Message

SUT	System Under Test
SVoIP	Secure Voice over Internet Protocol
SVoSIP	Secure Voice over Secure Internet Protocol
Sw	Switch
SW64	Switched 64 kbps
SWA	Southwest Asia
Syslog	System Log
SysLog	System Log
T	Ethernet Half-Duplex
T&S	Timing and Synchronization
TA	Terminal Adapter
~~TAU~~	~~Test Access Unit~~
TBD	To Be Determined
~~TC~~	~~Tandem Completing~~
TCA	Threshold Crossing Alert
~~TCA~~	~~Traffic Conditioning Agreement~~
TCAP	Transaction Capabilities Application Part
~~TCC~~	~~Telephony Country Code~~
TCCC	Theater C4I Coordination Center (EUCOM)
TCI	Tag Control Information
~~TCLt~~	~~Temporarily Weighted Terminal Coupling Loss~~
TCLw	Weighted Terminal Coupling Loss
~~TCM~~	~~Traveling Class Mark~~
TCP	Transmission Control Protocol
TCP	Transport Control Protocol
~~TDD~~	~~Telecommunications Devices for the Deaf~~
TDEA	Triple Data Encryption Algorithm
TDM	Time Division Multiplexing
~~TDM/P~~	~~Time Division Multiplexing/Packetized~~
TDMA	Time Division Multiple Access
~~TDR~~	~~Time Domain Reflectometry~~
TE	Terminal Equipment
TE	Traffic Engineering
TE1	Terminal Equipment Type 1
TE2	Terminal Equipment Type 2
~~TFC~~	~~Transfer Control~~
~~TFP~~	~~Transfer Prohibited~~
~~TFR~~	~~Transfer Restricted~~
TG	Trunk Gateway
TG	Trunk Group
~~THSDN~~	~~Tactical High Speed Digital Network~~

TIA	Telecommunications Industry Association
TIAS	Transport Independent Application-Specific
~~TID~~	~~Trunk ID~~
TIPHON	Telecommunications and Internet Protocol Harmonization over Networks
TISP	Tailored Information Support Plan
TJTN	Theater Joint Tactical Networks
TJTNCCB	Theater Joint Tactical Networks Configuration Control Board
~~TLP~~	~~Transmission Level Point~~
TLS	Transport Layer Security
TLV	Type-Length-Value
~~TLWS~~	~~Trunk and Line Workstation~~
~~TM~~	~~Technical Manual~~
TMR/USI	Transmission Medium Requirement/User Service Information
TN	Tactical-Edge Network
TNC	Theater Network Operations Center
T-NE	Tactical Network Element
TOC	Tactical Operations Center
TOD	Time of Day
~~ToIP~~	~~Text over IP~~
~~TOS~~	~~Trunk Out of Service~~
~~ToS~~	~~Type of Service~~
TOS	Type of Service
TPID	Tag Protocol Identification
TpoA	Transport Point of Attachment
~~TR~~	~~Technical Reference~~
~~TRD~~	~~Timed Release Disconnect~~
~~TRE~~	~~Trunk Reservation~~
Tri-Tac	Tri-Service Tactical Communications
TRN	Tactical Radio Network (needs expanded)
TS	Tandem Switch
TS/SCI	Top Secret/Sensitive Compartmented Information
TSA	Time Slot Assignment
TSAT	Transformational Communications Satellite System
~~TSC~~	~~Test System Controller~~
TSF	Transport Switching Function
TSGR	Transport Systems Generic Requirements (needs expanded)
TSI	Time Slot Interchange
~~TSP~~	~~Tandem Switching Provider~~
TSRD	Telecommunications Security Requirements Document
TSSI	Telecom Switched Services Interoperability
~~T-T~~	~~Tactical-to-Tactical~~

TTA	Telecommunication Technology Association
TTC	Telecommunication Technology Committee
TTL	Time to Live
~~TTY~~	~~Teletypewriter~~
TURN	Traversal Using Relay NAT
~~TW~~	~~True Wave~~
TWC	Three-Way Calling (needs expanded in text)
TX	Ethernet Full-Duplex
U	Unclassified
U.S.C.	United States Code
UA	User Agent
UAC	User Agent Client
U-AR	Unclassified Aggregation Router
UAS	Unavailable Seconds
UAS	User Agent Server
~~UAV~~	~~Unmanned Aerial Vehicle~~
UC	Unified Capabilities
UCCO	Unified Capabilities Connection Office
U-CE	Unclassified Customer Edge Router
UCR	Unified Capabilities Requirements
UCR 2007	Unified Capabilities Requirements 2007
UCR 2008	Unified Capabilities Requirements 2008
UCR 2010	Unified Capabilities Requirements 2010~~08~~
UCTP	Unified Capabilities Test Plan
UDP	User Datagram Protocol
UDT	Unitdata
UDTS	Unitdata Service
UFS	User Features and Services
UGS	Unsolicited Grant Service
UHF	Ultra High Frequency
UI	Unit Interval
UIpp	Unit Interval Peak-to-Peak
UIrms	Unit Interval Root Mean Square
~~ULCS~~	~~Unit Level Circuit Switch~~
~~UN~~	~~Uniform Numbering~~
UNI	User Network Interface
UPA	Unauthorized Precedence Announcement
U-PE	Unclassified Provider Edge
UPPS	User Provided Passed Screening
UPS	Uninterruptible Power Supply
UPSR	Unidirectional Path Switched Ring

UPU	User Part Unavailability
URI	Uniform Resource Identifier
~~URL~~	~~Uniform Resource Location~~
USF	User Service and Feature
USI	User Service Information
USM	User-Based Security Model
~~USTWC~~	~~Usage-Sensitive Three-Way Calling~~
~~UTC~~	~~Universal Time Coordinated~~
UTP	Unshielded Twisted Pair
V	Volt
VAD	Voice Activity Detection
VBD	Voice Band Data
VC	Virtual Circuit
VCA	Vacant Code Announcement
VCAT	Virtual Concatenation
VCFC	Video Channel Flow Control
VCFUR	Video Channel Fast Update Request
VCL	Video Coding Layer
VDC	Volt Direct Current (needs expanded in text)
VD-NE	Virtual Deployed Network Element
~~VDT~~	~~Video Display Terminal~~
VF	Voice Frequency
VG1	Voice Grade 1
VG2	Voice Grade 2
VG3	Voice Grade 3
VG4	Voice Grade 4
VG5	Voice Grade 5
VG6	Voice Grade 6
VHF	Very High Frequency
VID	VLAN Identification
VLAN	Virtual Local Area Network
VLR	Visitor Location Register
VMPS	VLAN Management Policy Server
~~VMS~~	~~Vulnerability Management System~~
~~VMWI~~	~~Visual Message Waiting Indicator~~
VNAR	Voice Net Access Radio
~~VoATM~~	~~Voice over Asynchronous Transfer Mode~~
VoIP	Voice over Internet Protocol
~~VOP~~	~~Voice over Packet~~
~~VoSIP~~	~~Voice over Secure Internet Protocol~~
VPIM	Voice Profile for Internet Mail

VPLS	Virtual Private LAN Service
VPN	Virtual Private Network
VP-P	Volts Peak-to-Peak (needs to be expanded in text)
VRRP	Virtual Router Redundancy Protocol
~~VSC~~	~~Vertical Service Code~~
VSR	Very Short Reach
VSU	Video ~~Switch~~ Session Unit
VT	Virtual Tributary
~~VT1.5~~	~~Virtual Tributary 1.5~~
VTC	Video Teleconferencing
VTCoIP	Video Teleconferencing over IP
~~VT-NE~~	~~Virtual Tactical Network Element~~
~~VToA~~	~~Voice Telephony over ATM~~
VTU	Video Teleconferencing Unit
VVoIP	Voice and Video over Internet Protocol
WAB	Wireless Access Bridge
WAN	Wide Area Network
~~W-ASAC~~	~~WAN Level ASAC~~
~~WATS~~	~~Wide Area Telecommunications Service~~
WD	Weather Day
WDCS	Wideband Digital Cross-connect System
WEI	Wireless End Instrument
WFQ	Weighted Fair Queuing
WG	Working Group
WIDS	Wireless Intrusion Detection System
WIN-T	Warfighter Information Network – Terrestrial
WLAN	Wireless Local Area Network
WLAS	Wireless LAN Access System
~~WLT~~	~~Wireline Terminal~~
WPA	Wi-Fi Protected Access
~~WPAN~~	~~Wireless Personal Area Network~~
WPS	Wireless Priority Service
WTR	Wait to Restore
WWNDP	World Wide Numbering and Dialing Plan (expand in text)
XML	Extensible Markup Language
XMPP	Extensible Messaging and Presence Protocol
XUDT	Extended Unitdata
XUDTS	Extended Unitdata Service

SECTION A4
REFERENCES

A4.1 AMERICAN NATIONAL STANDARDS INSTITUTE DOCUMENTATION

American National Standard Institute (ANSI), "Operations, Administration, Maintenance, and Provisioning Security Requirements for Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane," T1M1.5/2003-007R4, Draft Proposed April 1, 2003.

ANSI T1.101-1987 — *Synchronization Interface Standards for Digital Networks*, 1987

ANSI T1.102-1993 — *Digital Hierarchy – Electrical Interfaces*, December 1993.

ANSI T1.102-1999 — *Digital Hierarchy – Electrical Interfaces*, 1999.

ANSI T1.105-2001 — *Synchronous Optical Network (SONET) – Basic Description including Multiplex Structure, Rates, and Formats*, May 2001.

ANSI T1.105.1-2000 — *Synchronous Optical Network (SONET) – Automatic Protection*, Revised 2005.

ANSI T1.105.03-1994 — *Synchronous Optical Network (SONET) – Jitter Network Interfaces*, Revised 2008.

ANSI T1.105.03-2003 — *Synchronous Optical Network (SONET) – Jitter Network Interfaces*, Revised 2008.

ANSI T1.105.06-2002 — *Synchronous Optical Network (SONET) – Physical Layer Specifications*, Revised 2007.

ANSI T1.107-2002 — *Digital Hierarchy – Formats Specifications*, Revised 2006.

ANSI T1.111 — *Signaling System Number 7 (SS7) – Message Transfer Part (MTP)*, 2001.

ANSI T1.112 — *Signaling System Number 7 (SS7) – Signaling Connection Control Part (SCCP)*, 2001.

ANSI T1.113	*Signaling System No. 7 (SS7) – Integrated Services Digital Network (ISDN) User Part*, 1995.
ANSI T1.113-2000	*Signaling System No. 7 (SS7) – Integrated Services Digital Network (ISDN) User Part* (Revision of T1.113-1995; includes two Supplements: T1.113a-2000 and T1.113b-2001).
ANSI T1.113.3	*Signaling System No. 7 (SS7) – Signaling Link.*
ANSI T1.114	*Signaling System Number 7 (SS7) – Transaction Capabilities and Application Part (TCAP),* 2000.
ANSI T1.231-1993	*Digital Hierarchy - Layer 1 In-Service Digital Transmission Performance Monitoring,* 1993.
ANSI T1.231.01-2003	*Digital Subscriber Line (DSL) – Layer 1 In-Service Digital Transmission Performance Monitoring,* Revised 2007.
ANSI T1.403-1999	*Network to Customer Installation Interfaces – DS1 Electrical Interface,* Revised 2007.
ANSI T1.404-2002	*Network and Customer Installation Interfaces – DS3 Metallic Interface Specification* (Revision and Consolidation of T1.404-1994 and T1.404a-1996), Revised 2006.
ANSI T1.601-1999	*ISDN Basic Access Interface for Use on Metallic Loops for Application at the Network Side of NT, Layer 1 Specification*.
ANSI T1.602	*Data Link Layer Signalling Specification for Application at the User-Network Interface,* February 2000.
ANSI T1.605-1991 (1999)	*ISDN Basic Access Interface for S and T Reference Points and Layer 1 Specification*.
ANSI T1.607-1998	*ISDN Layer 3 Signaling Specifications for Circuit Switched Bearer Service for Digital Subscriber Signaling System No. 1 (DSS1).*
ANSI T1.613-1992	*ISDN Call Waiting Supplementary Service*.
ANSI T1.615-1992 (R1999)	*Digital Subscriber Signalling System No. 1 (DSS1)-Layer 3 Overview*.

ANSI T1.616-1992 *ISDN Call Hold Supplementary Service*.

ANSI T1.619-1992 (R2005) *Integrated Services Digital Network (ISDN) – Multi-Level Precedence and Preemption (MLPP) Service Capability*, February 1992, Reaffirmed 2005.

ANSI T1.619a-1994 (R1999) *Integrated Services Digital Network (ISDN) – Multi-Level Precedence and Preemption (MLPP) Service Capability (MLPP Service Domain and Cause Changes)*, July 1994, Reaffirmed 1999.

ANSI T1.621-1992 *ISDN User-to-User Signaling Supplementary Service*.

ANSI T1.632-1993 *ISDN Normal Call Transfer Supplementary Service*.

ANSI T1.642-1993 *ISDN Call Deflection Supplementary Service*.

ANSI T1.643-1995 *ISDN Explicit Call Transfer Supplementary Service*.

ANSI T1.647-1995 *ISDN Conference Calling Supplementary Service*.

ANSI T1.679-2004 *Interworking between Session Initiation Protocol (SIP) and Bearer Independent Call Control or ISDN User Part*, June 2004.

ANSI T1X1.3/94-001R5 *Jitter Measurement Methodology*.

ANSI X3.296 *Information Technology – Single-Byte Command Code Sets Connection (SBCON) Architecture*, Replaces ANSI X3.296-1997.

ANSI INCITS 230-1994 *Information Technology – Fibre Channel – Physical and Signaling Interface (FC-PH)*, (formerly ANSI X3.230-1994), Revised 2004.

ANSI INCITS 374-2003 *Information Technology – Fibre Channel – Single-Byte Command Code Sets Mapping Protocol – 3 (FC-SB-3)*, 2003.

ANSI/TIA-810-B *Telecommunications – Telephone Terminal Equipment – Transmission Requirements for Narrowband Voice over IP and Voice over PCM Digital Wireline Telephones*, SP-3-4352-RV2 (to become ANSI/TIA-810-B).

A4.2 BRITISH STANDARDS INSTITUTE DOCUMENTATION

BS EN 60950-1:2006 "Information technology equipment. Safety. General requirements," August 6, 2006.

A4.3 CHAIRMAN OF THE JOINT CHIEFS OF STAFF DOCUMENTATION

CJCSI 3170.01G "Joint Capabilities Integration and Development System," 1 March 2009.

CJCSI 6211.02C "Defense Information Systems Network (DISN): Policy and Responsibilities," 9 July 2008.

CJCSI 6212.01D "Interoperability and Supportability of Information Technology and National Security Systems," 8 March 2006, Current as of 14 March 2007.

CJCSI 6215.01C "Policy for Department of Defense (DoD) Voice Networks with Real Time Services (RTS)," 9 November 2007.

CJCSI 6215.02A "Policy, Responsibilities, Processes, and Administration for the Department of Defense Global Information Grid Networks," 31 July 2004.

CJCSI 6510.01E "Information Assurance (IA) and Computer Network Defense (CND)," 15 June 2004.

CJCSM 6231.02 "Manual for Employing Joint Tactical Communications Systems, Joint Voice Communications Systems," 01 August 1998.

CJCSM 6510.01 "Defense in Depth: Information Assurance (IA) and Computer Network Defense (CND)," 25 March 2003, Change 1, 10 August 2004, and Change 2, 26 January 2006.

A4.4 DEFENSE INFORMATION SYSTEMS AGENCY DOCUMENTATION

Defense Information Systems Agency "Global Information Grid (GIG) Convergence Master Plan (GCMP)," Version 5.25b, 29 March 2006.

Defense Information Systems Agency, DISAC 300-115-7, "Communications Security: Defense Red Switch Network (DRSN) Security Guidance," 19 February 2002.

Defense Information Systems Agency, DISAC 370-V130-1, 5 November 1965.

Defense Information Systems Agency, DISAC 310-255-1, "DSN User Services Guide," 21 April 1998.

DISA Field Security Operations, "DoD Instant Messaging Security Technical Implementation Guide," Version 1, Release 2, 15 February 2008.

DISA Field Security Operations, "DoD Personal Computer Communications Client (Voice/Video/Collaboration Security Technical Implementation Guide," Version 1, Release 1, 15 June 2008.

DISA Field Security Operations, "DoD Secure Telecommunications and Defense Red Switch Network Security Technical Implementation Guide," Version 1, Release 1, 28 March 2006.

DISA Field Security Operations, "DoD Telecommunications and Defense Switched Network Security Technical Implementation Guide," Version 2, Release 2, 30 June 2005.

DISA Field Security Operations, "Instant Messaging Checklist," Version 1, Release 1.3, February 15, 2008.

DISA Field Security Operations, "Network Infrastructure Security Technical Implementation Guide," Version 6, Release 4, 16 December 2005.

DISA Field Security Operations, "Personal Computer Communications Client (Voice/Video/Collaboration) Checklist," Version 1, Release 1.1, August 15, 2008.

DISA Field Security Operations, "Voice over Internet Protocol (VoIP) Security Technical Implementation Guide," Version 2, Release 1, 29 August 2005.

DISA Field Security Operations, "Wireless Security Technical Implementation Guide."

"Initial Capabilities Document for Global Information Grid 2.0 (GIG 2.0)," May 29, 2009.

Defense Information Systems Agency, "Defense Information Systems Agency (DISA) Campaign Plan."

Defense Information Systems Agency, "DISN Overarching Technical Strategy (DOTS)."

Defense Information Systems Agency, "DISN Technology Evolution Plan (DTEP)."

A4.5 DEPARTMENT OF DEFENSE DOCUMENTATION

"Department of Defense (DoD) Class 3 Public Key Infrastructure (PKI) Public Key-Enabled Application Requirements," Version 1.0, 13 July 2000.

"Department of Defense (DoD) Unified Capabilities (UC) Master Plan (UC MP)," December 15, 2009.

DoD CIO, "Department of Defense Global Information Grid Architectural Vision: Vision for a Net-Centric, Service-Oriented DoD Enterprise," Version 1, June 2007.

DoD CIO Guidance IA6-8510 IA.

"Department of Defense Joint Technical Architecture (JTA)," Version 6.0, 3 October 2003.

"DoD Architecture Framework Version 1.0," February 8, 2004.

"The Global Information Grid (GIG) ~~Net-Centric Implementation Document (NCID) V2.0: T300, Quality of Service," December 2005~~Enterprise Service Profile.

Center for DISN Services, "DISN Service Level Agreement for the Defense Information Systems Agency and its customers."

Common Criteria Evaluation and Validation Scheme, 6 August 2004.

Department of Defense Assured Service Session Initiation Protocol (AS-SIP) Generic System Requirement (GSR), Defense Information Systems Agency, Version 1.2.1, 12 May 2006.

Department of Defense Real Time Services (RTS) Information Assurance (IA) Generic System Requirement (GSR), Defense Information Systems Agency, Revision 1.4, 8 September 2006.

Department of Defense Real-Time Services (RTS) Generic System Requirements (GSR) and Generic System Specifications (GSS) Appendices Overview, Revision 0.2, 16 August 2006.

Department of Defense Voice Networks Generic Switching Center Requirements (GSCR), 8 September 2003, ERATA Change 1, 1 March 2005.

Department of Defense Wide Area Network (WAN) Generic System Requirement (GSR), Defense Information Systems Agency, Revision 1.3, 18 May 2006.

Deputy Assistant Secretary of Defense (Deputy CIO), "DSN Generic Switching Center Specification (GSCR)," signed by the Deputy Assistant Secretary of Defense (Deputy CIO), September 8, 2003.

Deputy Secretary of Defense, "Smart Card Adoption and Implementation," 10 November 1999.

DoD 8910.1-M, "DoD Procedures for Management of Information Requirements," 30 June 1998.

"DoD Architecture Framework," Version 1.0, 8 February 2004.

DoD CIO Memorandum, "Internet Protocol Version 6 (IPv6) Interim Transition Guidance," 29 September 2003.

DoD CIO Memorandum, "Internet Protocol Version 6 (IPv6)," 9 June 2003.

DoD CIO Memorandum "DoD IPv6 Definitions," 26 June 2008.

DoD Information Technology Standards Registry (DISR) IPv6 Standards Technical Working Group (TWG), "DoD IPv6 Standard Profiles for IPv6 Capable Products," Version 1.0, 1 June 2006.

DoD Real Time Services Working Group, "DoD RTS IA Countermeasures," 29 March 2006.

DoD RTS IA Working Group, "Analysis of Information Assurance Requirements and Threats for the DoD Real-Time Services Environment Version 3.4," 23 May 2006.

"DoD Voice Networks Generic Switching Center Requirements (GSCR)," 8 September 2003, Errata Change 1, 1 March 2005.

DSN Systems Design, Implementation, and Transition Branch, "Defense Switched Network (DSN) IPv6 Transition Plan," Version 1.1, 28 June 2006.

Interim Department of Defense (DoD) Certification and Accreditation (C&A) Process Guidance, "DoD Information Assurance Certification and Accreditation Process (DIACAP)," July 6, 2006.

Office of DoD CIO, "DoD Internet Protocol Version 6 (IPv6) Transition Plan," Version 1.0, November 2003.

United States Strategic Command (STRATCOM), "Joint Concept of Operations for Global Information Grid Network Operations (NetOps)," 20 April 2004.

Director of Central Intelligence Directive (DCID) 6/3, "Protecting Sensitive Compartmented Information within Information Systems," 5 June 1999.

A4.6 DOD DIRECTIVES

DoDD 4630.05 "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," 11 January 2002, Certified current as of 23 April 2007.

DoDD 5000.01 "The Defense Acquisition System," 12 May 2003, Certified current as of 20 November 2007.

DoDD 5144.1 "Assistant Secretary of Defense for Networks and Informaiton Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO)," May 2, 2005.

DoDD 5200.28 "Security Requirements for Automated Information Systems (AISs)," 21 March 1988.

DoDD 8000.01 "Management of the Department of Defense Information Enterprise," February 10, 2009.

DoDD 8100.1 "Global Information Grid (GIG) Overarching Policy," 19 September 2002, Certified Current as of November 21, 2003.

DoDD 8115.01 "Information Technology Portfolio Management," 10 October 2005.

DoDD 8500.01E "Information Assurance (IA)," October 24, 2002, Certified Current as of April 23, 2007.

DoDD 8530.1 "Computer Network Defense," 8 January 2001.

A4.7 DOD INSTRUCTIONS

DoDI 4630.8 "Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," 30 June 2004.

DoDI 5000.02 "Operation of the Defense Acquisition System," 8 December 2008.

DoDI 5200.40 "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," 30 December 1997.

DoDI 8100.ee "Department of Defense Unified Capabilities," Draft, October 2009.

DoDI 8100.3 "Department of Defense (DoD) Voice Networks," 16 January 2004.

DoDI 8410.02 "DoD NetOps for the Global Information Grid (GIG)," 19 December 2008.

DoDI 8500.2 "Information Assurance (IA) Implementation," 6 February 2003.

DoDI 8510.01 "DoD Information Assurance (IA) Certification and Accreditation Process (DIACAP)," 28 November 2007.

DoDI 8551.1 "Ports, Protocols, and Services Management (PPSM)," 13 August 2004.

A4.8 ETSI DOCUMENTATION

EN 50022 "Specification for low voltage switchgear and controlgear for industrial gear," 1977.

EN 50082
ETS-FN-50022 "Electromagnetic compatibility. Generic immunity standard. Residential, commercial and light industry," January 1998.

ETS 300 019 "Equipment Engineering (EE); Environmental Conditions and Environmental Tests for Telecommunications Equipment," 1994.

EN 300 386 "Electromagnetic compatibility and Radio spectrum Matters (ERM); Telecommunication network equipment; ElectroMagnetic Compatibility (EMC) requirements," Edition 1.3.1, September 1, 2001.

TS 102 165-1 "Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN) – Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis," Version 4.2.1, December 2006.

TS 102 165-2 "Telecommunications and Internet Protocol Harmonization over Networks (TIPHON) Release 4; Protocol Framework Definition; Methods and Protocols for Security; Part 2: Counter Measures," Version 4.1.1, February 2003.

TS 183 029 Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN simulation services: Explicit Communication Transfer (ECT); Protocol specification, Version 2.5.0.

A4.9 FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATIONS

FIPS PUB 140-2 U.S. Department of Commerce/National Institute of Standards and Technology, "Security Requirements for Cryptographic Modules," 25 May 2001.

FIPS PUB 186-2 U.S. Department of Commerce/National Institute of Standards and Technology, "Digital Signature Standard (DSS)," 27 January 2000.

FIPS 197 Federal Information Processing Standards Publication 197, "Advanced Encryption Standard (AES)," 26 November 2001.

A4.10 INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, INC. DOCUMENTATION

IEEE 455-1985 IEEE Standard for Standard Test Procedure for Measuring Longitudinal Balance of Telephone Equipment Operating in the Voice Band, 1 January 2001.

IEEE 802.1D™-2004 IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges, June 2004.

IEEE 802.1Q™-1998 IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks, 1 January 1998.

IEEE 802.1Q™-2003 IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks, 2003.

IEEE 802.1s IEEE Standard for Local and Metropolitan Area Networks: Multiple Spanning Trees, 2003. (Merged into 802.1Q-2003).

IEEE 802.1w IEEE Standard for Local and Metropolitan Area Networks: Rapid Reconfiguration of Spanning Tree, 2003. (Merged into 802.1D-2004).

IEEE 802.1X™-2001 IEEE Standard for Local and Metropolitan Area Networks: Port Based Network Access Control, 2001.

IEEE 802.3™-1993 IEEE Standard for information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications, 1993.

IEEE 802.3™-2008 IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications, December 26, 2008.

IEEE 802.3i IEEE Standard for information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications: 10BASE-T 10 Mbit/s (1.25 MB/s) over twisted pair, 1990.

IEEE 802.3u-1995 IEEE Standard for information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications: 100BASE-TX, 100BASE-T4, 100BASE-FX Fast Ethernet at 100 Mbit/s (12.5 MB/s) w/autonegotiation, 1995.

IEEE 802.3x-1997 IEEE Standard for information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications: Full Duplex and flow control, 1997.

IEEE 802.3z-1998 IEEE Standard for information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications: 1000BASE-X Gbit/s Ethernet over Fiber-Optic at 1 Gbit/s (125 MB/s), 1998.

IEEE 802.3ab-1999 IEEE Standard for information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications: 1000BASE-T Gbit/s Ethernet over twisted pair at 1 Gbit/s (125 MB/s), 1999.

IEEE 802.3ad-2000 IEEE Standard for information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications: Link aggregation for parallel links, 2000.

IEEE 802.3ae-2003 IEEE Standard for information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications: 10 Gbit/s (1,250 MB/s) Ether over fiber; 10GBASE-SR, 10GBASE-LR, 10GBASE-ER, 10GBASE-SW, 10GBASE-LW, 10GBASE-EW, 2003.

IEEE 802.11™-2007 IEEE Standard for information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, June 2007.

IEEE 802.11a Supplement to IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: High-speed Physical Layer in the 5 GHz Band, June 2003.

IEEE 802.11b Supplement to IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band, June 2003.

IEEE 802.11e Supplement to IEEE Standard for Information technology—Telecommunications and information exchange between systems—

Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Wireless LAN for Quality of Service, June 2003.

IEEE 802.11e-2005 — Supplement to IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 8, Medium Access Control (MAC) Quality of Service Enhancements, February 09, 2006.

IEEE 802.11h — Supplement to IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 5, December 29, 2003.

IEEE 802.11i — Supplement to IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 6, Medium Access Control (MAC), February 14, 2005.

IEEE 802.11g — Supplement to IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band, June 2003.

IEEE 802.16™-2004 — IEEE Standard for Local and metropolitan area networks—Part 16: Air Interface for Fixed Broadband Wireless Access Systems, 1 October 2004.

IEEE 802.16d™ — Standard for Amendment to IEEE Standard for Local and metropolitan area networks - Part 16: Air Interface for Fixed Broadband Wireless Access Systems - Detailed System Profiles for 2-11 GHz, December 11, 2002.

IEEE 802.16e™ IEEE Standard for Local and metropolitan area networks— Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems, Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands *and* Corrigendum 1, 28 February 2006.

IEEE 802.17-2004 IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements - Part 17: Resilient Packet Ring (RPR) Access Method and Physical Layer Specifications, September 24, 2004.

A4.11 INTERNATIONAL TELECOMMUNICATION UNION DOCUMENTATION

E.164 ITU-T Recommendation E.164, "The International Public Telecommunication Numbering Plan," Geneva, Switzerland, 2005.

~~E.721 ITU-T Recommendation E.721, "Network grade of service parameters and target values for circuit-switched services in the evolving ISDN," Geneva, Switzerland, May 1999.~~

G.107 ITU-T Recommendation G.107, "The E-model: a computational model for use in transmission planning," Geneva, Switzerland, April 2009.

G.165 ITU-T Recommendation G.165, "Echo cancellers," Geneva, Switzerland, November 1988.

G.168 ITU-T Recommendation G.168, "Digital network echo cancellers," Geneva, Switzerland, January 2007.

G.651 ITU-T Recommendation G.651, "Characteristics of a 50/125 µm multimode graded index optical fibre cable," February 1998.

G.651.1 ITU-T Recommendation G.651.1, "Characteristics of a 50/125 µm multimode graded index optical fibre cable for the optical access network," Geneva, Switzerland, July 2007.

G.652 ITU-T Recommendation G.652, "Characteristics of a single-mode optical fibre and cable," Geneva, Switzerland, June 2005.

G.655 ITU-T Recommendation G.655, "Characteristics of a non-zero dispersion-shifted single-mode optical fibre and cable," Geneva, Switzerland, March 2006.

G.691 ITU-T Recommendation G.691, "Optical interfaces for single channel STM-64 and other SDH systems with optical amplifiers," Geneva, Switzerland, March 2006.

~~G.692 ITU-T Recommendation G.692, "Optical Interfaces for Multichannel Systems with Optical Amplifiers," Geneva, Switzerland, October 1998.~~

G.693 ITU-T Recommendation G.693, "Optical interfaces for intra-office systems," Geneva, Switzerland, May 2006.

G.694.1 ITU-T Recommendation G.694.1, "Spectral grids for WDM applications: DWDM frequency grid," Geneva, Switzerland, 2002.

~~G.694.1 ITU-T Recommendation G.694.1, "Spectral grids for WDM applications: DWDM frequency grid," Geneva, Switzerland, June 2002.~~

G.703 ITU-T Recommendation G.703, "Physical/Electrical Characteristics of Hierarchical Digital Interfaces at 1544, 2048, 8448, and 44736 kbit/s Hierarchical Levels," 2001.

G.704 ITU-T Recommendation G.704, "Series G: Transmission Systems and Media, Digital Systems and Networks—Digital transmission systems – Terminal equipments – General Synchronous frame structures used at 1544, 6312, 2048, 8448 and 44 736 kbit/s hierarchical levels," October 1998.

G.707/ Y.1322 ITU-T Recommendation G.707/Y.1322, "Network node interface for the synchronous digital hierarchy (SDH)," Geneva, Switzerland, January 2007.

G.709/ Y.1331 ITU-T Recommendation G.709/Y.1331, "Network node interface for the optical transport network (OTN)," Geneva, Switzerland, March 2003.

G.711 ITU-T Recommendation G.711, "General Aspects of Digital Transmission Systems, Terminal Equipments, Pulse code modulation (PCM) of voice frequencies," Geneva, Switzerland, November 1988.

Appendix I, "A high quality low complexity algorithm for packet loss concealment with G.711," Geneva, Switzerland, September 1999.

Appendix II, "A comfort noise payload definition for ITU-T G.711 use in packet-based multimedia communication systems," Geneva, Switzerland, February 2000.

G.722 ITU-T Recommendation G.722, "7 kHz audio-coding within 64 kbit/s," Geneva, Switzerland, November 1988.

G.723.1 ITU-T Recommendation G.723.1, "Dual rate speech coder for multimedia communications transmitting at 5.3 and 6.3 kbit/s," Geneva, Switzerland, May 2006.

G.726 ITU-T Recommendation G.726, "32 kbps Adaptive Differential Pulse Code Modulation (ADPCM)," Geneva, Switzerland, December 1990.

G.728 ITU-T Recommendation G.728, "Coding of speech at 16 kbit/s using low-delay code excited linear prediction," Geneva, Switzerland, September 1992.

G.729 ITU-T Recommendation G.729, "Coding of speech at 8 kbit/s conjugate-structure algebraic-code-excited linear prediction (CS-ACELP)," Geneva, Switzerland, March 1996, plus Erratum 1, April 2006, and Annexes A through J, and Appendices I, II, and III.

G.729.1 ITU Recommendation G.729.1 (2006) Amendment 1, "New Annex A on G.729.1 usage in H.245, plus corrections to the main body and updated test vectors," Geneva, Switzerland, January 2007.

This corrigendum was never published, its content having been included in the published ITU-T Recommendation G.729.1 (2006)

G.729.1 ITU Recommendation G.729.1 (2006), "G.729 based Embedded Variable bit-rate codor: An 8-32 kbit/s scalable wideband coder bitstream interoperable with G.729," Geneva, Switzerland, May 2006.

This edition includes the modifications introduced by G.729.1 (2006) Amd. 1 approved on 13 January 2007, and G.729.1 (2006) Amd. 2 approved on 13 February 2007.

G.732 ITU-T Recommendation G.732, "Characteristics of primary PCM multiplex equipment operating at 2048 kbit/s," Geneva, Switzerland, November 1988.

~~G.772 ITU-T Recommendation G.772 (REV), "Protected monitoring points on digital transmission systems," Geneva, Switzerland, March 2003.~~

G.783 ITU-T Recommendation G.783, "Characteristics of synchronous digital hierarchy (SDH) equipment functional blocks," Geneva, Switzerland, March 2006.

G.811 ITU-T Recommendation G.811, “Timing characteristics of primary reference clocks,” 1997.

G.825 ITU-T Recommendation G.825, “The control of jitter and wander within digital networks which are based on the synchronous digital hierarchy (SDH),” Geneva, Switzerland, March 2003.

G.826 ITU-T Recommendation G.826, “End-to-end error performance parameters and objectives for international, constant bit-rate digital paths and connections,” Geneva, Switzerland, December 2002.

G.829 ITU-T Recommendation G.829, “Error performance events for SDH multiplex and regenerator sections,” Geneva, Switzerland, December 2002.

G.831 ITU-T Recommendation G.831, “Management capabilities of transport networks based on the synchronous digital hierarchy (SDH),” Geneva, Switzerland, March 2000.

G.841 ITU-T Recommendation G.841, “Types and characteristics of SDH network protection architectures,” Geneva, Switzerland, October 1998.

G.842 ITU-T Recommendation G.842, “Interworking of SDH network protection architectures,” Geneva, Switzerland, April 1997.

G.872 ITU-T Recommendation G.872, “Architecture of optical transport networks,” Geneva, Switzerland, November 2001.

G.957 ITU-T Recommendation G.957, “Optical interfaces for equipments and systems relating to the synchronous digital hierarchy,” Geneva, Switzerland, March 2006.

G.958 ITU-T Recommendation G.958, “Digital line systems based on the synchronous digital hierarchy for use on optical fibre cables.” [Withdrawn]

G.1070 ITU-T Recommendation G.1070, “Opinion model for video-telephony applications,” Geneva, Switzerland, April 2007.

G.7041/ Y.1303 ITU-T Recommendation G.7041/Y.1303, “Generic framing procedure (GFP),” Geneva, Switzerland, Geneva, Switzerland, October 2008.

G.7042/ Y.1305 ITU-T Recommendation G.7042/Y.1305, “Link capacity adjustment scheme (LCAS) for virtual concatenated signals,” Geneva, Switzerland, March 2006.

G.7043 Y.1343 ITU-T Recommendation G.7043/Y.1343, **"**Virtual concatenation of plesiochronous digital hierarchy (PDH) signals," Geneva, Switzerland, July 2004.

G.8251 ITU-T Recommendation G.8251(G.otnjit), "The control of jitter and wander within the optical transport network (OTN)," Geneva, Switzerland, November 2001.

H.224 ITU-T Recommendation H.224, "A real time control protocol for simplex applications using the H.221 LSD/HSD/MLP channels," Geneva, Switzerland, January 2005.

H.244 ITU Recommendation H.244, "Synchronized aggregation of multiple 64 or 56 kbit/s channels," Geneva, Switzerland, July 1995.

H.248.1 ITU-T Recommendation H.248.1, "Gateway control protocol: Version 3," Geneva Switzerland, September 2005.

H.248.24 ITU-T Recommendation H.248.24, "Gateway control protocol: Multi-frequency tone generation and detection packages," Geneva, Switzerland, July 2003.

H.248.25 ITU-T Recommendation H.248.24, "Gateway control protocol: Basic CAS packages," Geneva, Switzerland, January 2007.

H.248.28 ITU-T Recommendation H.248.28, "Gateway control protocol: International CAS packages," Geneva, Switzerland, January 2007.

H.261 ITU-T Recommendation H.261, "Video codec for audiovisual services at p x 64 kbit/s," Recommendation H.261, Geneva, Switzerland, March 1993.

H.263 ITU-T Recommendation H.263, "Video coding for low bit rate communication," Geneva, Switzerland, January 2005. (H.263a, H.323+, H.263 (1999)).

H.264 ITU-T Recommendation H.264, "Advanced video coding for generic audiovisual services," Geneva, Switzerland, March 2005. (Also, known as H.264/AVC)

H.281 ITU-T Recommendation H.281, "A far end camera control protocol for videoconferences using H.224," Geneva, Switzerland, November 1994.

H.320 ITU-T Recommendation H.320, "Narrow-band visual telephone systems and terminal equipment," Geneva, Switzerland, March 2004.

H.323 ITU-T Recommendation H.323, "Packet-based multimedia communications systems," Geneva, Switzerland, June 2006.

M.2101 ITU-T Recommendation M.2101, "Performance limits for bringing-into-service and maintenance of international multi-operator SDH paths and multiplex sections," Geneva, Switzerland, June 2003.

M.3100 ITU-T Recommendation M.3100, "Generic network information model," Geneva, Switzerland, April 2005.

~~P.561 ITU-T Recommendation P.561, "In-service non-intrusive measurement device – Voice service measurements," Geneva, Switzerland, July 2002.~~

~~P.562 ITU-T Recommendation P.562, "Analysis and interpretation of INMD voice-service measurements," Geneva, Switzerland, May 2004.~~

P.563 ITU-T Recommendation P.563, "Single Ended Method for Objective Speech Quality Assessment in Narrow-Band Telephony Applications", Geneva, Switzerland, April 2004

P.800.1 ITU-T Recommendation P.800.1, "Mean Opinion Score Technology," Geneva, Switzerland, March 2003

P.862 ITU-T Recommendation P.862, "Perceptual evaluation of speech quality (PESQ): An objective method for end-to-end speech quality assessment of narrow-band telephone networks and speech codecs," Geneva, Switzerland, February 2001.

Q.735.3 ITU-T Recommendation Q.735.3, "Stage 3 description for community of interest supplementary services using Signalling System No. 7: Multi-level precedence and preemption," Geneva, Switzerland, March 1993.

Q.850 ITU-T Recommendation Q.850, "Usage of cause and location in the Digital Subscriber Signalling System No. 1 and the Signalling System No. 7 ISDN User Part," Geneva, Switzerland, May 1998.

Q.921 ITU-T Recommendation Q.921, "ISDN user-network interface – Data link layer specification," Geneva, Switzerland, September 1997.

NOTE: This Recommendation is published with the double number Q.921 and I.441.

Q.931 ITU-T Recommendation Q.931, "ISDN user-network interface layer 3 specification for basic call control," Geneva, Switzerland, May 1998.

NOTE: This Recommendation is also included but not published in I series under alias number I.451.

Q.955.3 ITU-T Recommendation Q.955.3, "Stage 3 description for community of interest supplementary services using DSS 1 – Multi-level precedence and preemption (MLPP)," Geneva, Switzerland, March 1993.

Q.1912.5 ITU-T Recommendation Q.1912.5, "Interworking between Session Initiation Protocol (SIP) and Bearer Independent Call Control Protocol or ISDN User Part," Geneva, Switzerland, March 2004.

T.4 ITU-T Recommendation T.4, "Standardization of Group 3 facsimile terminals for document transmission," Geneva, Switzerland, July 2003.

T.38 ITU-T Recommendation T.38, "Procedures for real-time Group 3 facsimile communication over IP networks," Geneva, Switzerland, April 2007.

V.14 ITU-T Recommendation V.14, "Transmission of start-stop characters over synchronous bearer channels," Geneva, Switzerland, March 1993.

V.24 ITU-T Recommendation V.24, "List of definitions for interchange circuits between data terminal equipment (DTE) and data circuit-terminating equipment (DCE)," Geneva, Switzerland, February 2000.

V.32 ITU-T Recommendation V.32, "A family of 2-wire, duplex modems operating at data signalling rates of up to 9600 bit/s for use on the general switched telephone network and on leased telephone-type circuits," Geneva, Switzerland, March 1993.

V.34 ITU-T Recommendation V.34, "A modem operating at data signalling rates of up to 33 600 bit/s for use on the general switched telephone network and on leased point-to-point 2-wire telephone-type circuits," Geneva, Switzerland, February 1998.

V.35 ITU-T Recommendation V.35, "Data transmission at 48 kilobits per second using 60-108 kHz group band circuits," Geneva, Switzerland, October 1984.

V.54 ITU-T Recommendation V.54, "Loop test devices for modems," Geneva, Switzerland, November 1988.

V.90 ITU-T Recommendation V.90, "A digital modem and analogue modem pair for use on the Public Switched Telephone Network (PSTN) at data signalling rates of up to 56 000 bit/s downstream and up to 33 600 bit/s upstream," Geneva, Switzerland, September 1998.

V.92 ITU-T Recommendation V.92, "Enhancements to Recommendation V.90," November 2000.

V.150.1 ITU-T Recommendation V.150.1, "Modem-over-IP networks: Procedures for the end-to-end connection of V-series DCEs," Geneva, Switzerland, January 2003.

ITU-T Recommendation V.150.1, Amendment 1, Geneva, Switzerland, January 2005.

X.731 ITU-T Recommendation X.731, "Information technology – Open Systems Interconnection – Systems management: State management function," Geneva, Switzerland, January 1992.

X.805 ITU-T Recommendation X.805, "Security architecture for systems providing end-to-end communications," Geneva, Switzerland, October 2003.

Y.1540 ITU-T Recommendation Y.1540, "Internet protocol data communication service - IP packet transfer and availability performance parameters," November 2007.

Y.1541 ITU-T Recommendation Y.1541, "Network performance objectives for IP-based services," Geneva, Switzerland, February 2006.

A4.12 INTERNET ENGINEERING TASK FORCE REQUESTS FOR COMMENT

RFC 768 Postel, J., "User Datagram Protocol," August 1980.

RFC 791 Information Services Institute, "Internet Protocol," September 1981.

RFC 793 Information Services Institute, "Transmission Control Protocol," September 1981.

RFC 1046 Prue, W. and J. Postel, "A Queuing Algorithm to Provide Type-of-Service for IP Links," February 1988.

RFC 1142 Oran, D., Ed., "OSI IS-IS Intra-domain Routing Protocol," February 1990.

RFC 1157 Case, J., M. Fedor, M. Schoffstall, and J. Davin, "A Simple Network Management Protocol (SNMP)," May 1990.

RFC 1213 "Management Information Base for Network Management of TCP/IP-based internets: MIB-II"

RFC 1215 Rose, M., Ed., "A Convention for Defining Traps for use with SNMP," March 1991.

RFC 1629 Colella, R., R. Callon, E. Gardner and Y. Rekhter, "Guidelines for OSI NSAP Allocation in the Internet," May 1994.

RFC 1662 Simpson, W., Ed., "PPP in HDLC-like Framing," July 1994.

RFC 1772 Rekhter, Y., P. Gross, "Application of the Border Gateway Protocol in the Internet," March 1995.

RFC 1812 Baker, F., Ed., "Requirements for IP Version 4 Routers," June 1995.

RFC 1883 Deering, S., R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification," December 1995.

RFC 1918 Rekhter, Y., B. Moskowitz, D. Karrenberg, G. J. De Groot, and E. Lear, "Address Allocation for Private Internets," February 1996.

RFC 1981 McCann, J., S. Deering, and J. Mogul, "Path MTU Discovery for IP Version 6," August 1996.

RFC 1997 Chandra, R., P. Traina, and T. Li, "BGP Communities Attribute," August 1996.

RFC 2119 Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," March 1997.

RFC 2131 Droms, R., "Dynamic Host Configuration Protocol," March 1997.

RFC 2198 Perkins, C, I. Kouvelas, O. Hodson, V. Hardman, M. Handley, J.C. Bolot, A. Vega-Garcia, and S. Fosse-Parisis, "RTP Payload for Redundant Audio Data," September 1997.

RFC 2205 Braden, R., Ed., L. Zhang, S. Berson, S. Herzog, and S. Jamin, "ReSerVation Protocol (RSVP)–Version 1 Functional Specification," September 1997.

RFC 2206 Baker, F., J. Krawczyk, and A. Sastry, "RSVP Management Information Base using SMIv2," September 1997.

RFC 2210 Wroclawski, J., "The Use of RSVP with IETF Integrated Services," September 1997.

RFC 2211 Wroclawski, J., "Specification of the Controlled-Load Network Element Service," September 1997.

RFC 2212 Shenker, S., C. Partridge, and R. Guerin, "Specification of Guaranteed Quality of Service," September 1997.

RFC 2327 Handley, M. and V. Jacobson, "SDP: Session Description Protocol," April 1998.

RFC 2328 Moy, J., "OSPF Version 2," April 1998.

RFC 2362 Estrin, D., D. Farinacci, A. Helmy, D. Thaler, S. Deering, M. Handley, V. Jacobson, C. Liu, P. Sharma, and L. Wei, "Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification," June 1998.

RFC 2365 Meyer, D., "Administratively Scoped IP Multicast," July 1998.

RFC 2385 Heffernan, A., "Protection of BGP Sessions via the TCP MD5 Signature Option," August 1998.

RFC 2401 Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol," November 1998.

RFC 2404 Madson, C. and R. Glenn, "The Use of HMAC-SHA-1-96 within ESP and AH," November 1998.

RFC 2407 Piper, D., "The Internet IP Security Domain of Interpretation for ISAKMP," November 1998.

RFC 2408 Maughan, D., M. Schertler, M. Schneider and J. Turner, "Internet Security Association and Key Management Protocol (ISAKMP)," November 1998.

RFC 2409 Harkins, J. and D. Carrel, "The Internet Key Exchange (IKE)," November 1998.

RFC 2427 Brown, C. and A. Malis, "Multiprotocol Interconnect over Frame Relay," September 1998.

RFC 2439 Villamizar, C., R. Chandra, and R. Govindan, "BGP Route Flap Damping," November 1998.

RFC 2460 Deering S. and R. Hinden, "Internet Protocol Version 6 (IPv6) Specification," December 1998.

RFC 2461 Narten, T., E. Nordmark, and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)," December 1998.

RFC 2462 Thomson, S. and T. Narten, "IPv6 Stateless Address Autoconfiguration," December 1998.

RFC 2464 Crawford, M., "Transmission of IPv6 Packets over Ethernet Networks," December 1998.

RFC 2472 Haskin, D. and E. Allen, "IP Version 6 over PPP," December 1998.

RFC 2473 Conta, A. and S. Deering, "Generic Packet Tunneling in IPv6 Specification," December 1998.

RFC 2474 Nichols, K., S. Blake, F. Baker, and D. Black, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers," December 1998.

RFC 2475 Blake, S., D. Black, M. Carlson, E. Davies, Z. Wang, and W. Weiss, "An Architecture for Differentiated Services," December 1998.

RFC 2494 Fowler, D., Ed., "Definitions of Managed Objects for the DS0 and DS0 Bundle Interface Type," January 1999.

RFC 2543 Handley, M., H. Schulzrinne, E. Schooler, J. Rosenberg "SIP: Session Initiation Protocol," March 1999.

RFC 2545 Marques, P. and F. Dupont, "Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing," March 1999.

RFC 2547 Rosen, E. and Y. Rekhter, "BGP/MPLS VPNs," March 1999.

RFC 2578 McCloghrie, K., D. Perkins, and J. Schoenwaelder, "Structure of Management Information Version 2 (SMIv2)," April 1999.

RFC 2579 McCloghrie, K., D. Perkins, and J. Schoenwaelder, "Textual Conventions for SMIv2," April 1999.

RFC 2580 McCloghrie, K., D. Perkins, and J. Schoenwaelder, "Conformance Statements for SMIv2," April 1999.

RFC 2597 Heinanen, J., F. Baker, W. Weiss, and J. Wroclawski, "Assured Forwarding PHB Group," June 1999.

RFC 2660 Rescorla, E., and A. Schiffman, "The Secure HyperText Transfer Protocol," August 1999.

RFC 2684 Grossman, D, and J. Heinanem, "Multiprotocol Encapsulation over ATM Adaptation Layer 5," September 1999.

RFC 2685 Fox, B., B. Gleeson, "Virtual Private Networks Identifier," September 1999.

RFC 2702 Awduche, D., J. Malcolm, J. Agogbua, M. O'Dell, and J. McManus, "Requirements for Traffic Engineering Over MPLS," September 1999.

RFC 2710 Deering S., W. Feener, and B. Haberman, "Multicast Listener Discovery (MLD) for IPv6," October 1999.

RFC 2711 Partridge, C. and A. Jackson, "IPv6 Router Alert Option," October 1999.

RFC 2740 Coltun, R., D. Ferguson, and J. Moy, "OSPF for IPv6," December 1999.

RFC 2747 Baker, F., Lindell, B., Talwar, M., "RSVP Cryptographic Authentication," January 2000.

RFC 2784 Farinacci, D., T. Li, S. Hanks, D. Meyer, and P. Traina, "Generic Routing Encapsulation (GRE)," March 2000.

RFC 2787 Jewell, B., "Definitions of Managed Objects for the Virtual Router Redundancy Protocol," March 2000.

RFC 2805 Greene, N., M. Ramalho, and B. Rosen, "Media Gateway Control Protocol Architecture and Requirements," RFC 2805, April 2000.

RFC 2818 Rescorla, E., "HTTP over TLS, May 2000.

RFC 2819 Waldbusser, S., "Remote Network Monitoring Management Information Base," May 2000.

RFC 2833 Schulzrinne, H. and S. Petrack, "RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals," May 2000.

RFC 2858 Bates, T., Y. Rekhter, R. Chandra, and D. Katz, "Multiprotocol Extensions for BGP-4," June 2000.

RFC 2866 Rigney, C., "RADIUS Accounting," June 2000.

RFC 2917 Muthukrishnan, K. and A. Malis, "A Core MPLS IP VPN Architecture," September 2000.

RFC 2961 Berge, L., Gan, D., Swallow, G., Pan, P., Tommasi, F., Molendini, S., "RSVP Refresh Overhead Reduction Extensions," April 2001.

RFC 2973 Balay, R., Katz, D., Parker, J., "IS-IS Mesh Groups," October 2000.

RFC 2976 Donovan, S., "The SIP INFO Method," October 2000.

RFC 3031 Rosen, E., A. Viswanathan, and R. Callon, "Multiprotocol Label Switching Architecture," January 2001.

RFC 3032 Rosen, E., D. Tappan, G. Fedorkow, Y. Rekter, D. Farinacci, T. Li, and A. Conta, "MPLS Label Stack Encoding," January 2001.

RFC 3036 Andersson, L., P. Doolan, N. Feldman, A. Fredette, and B. Thomas, "LDP Specification," January 2001.

RFC 3037 Thomas, B. and E. Gray, "LDP Applicability," January 2001.

RFC 3041 Narten, T. and R. Draves, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6," January 2001.

RFC 3053 Durand, A., P. Fasano, I. Guardini, and D. Lento, "IPv6 Tunnel Broker," January 2001.

RFC 3107 Rekhter, Y. and E. Rosen, "Carrying Label Information in BGP-4," May 2001.

RFC 3118 Droms, R., Ed., W. Arbaugh, "Authentication for DHCP Messages," June 2001.

RFC 3140 Black, D., S. Brim, B. Carpenter, and F. Le Faucheur, "Per Hop Behavior Identification Codes," June 2001.

RFC 3162 Aboba, B., G. Zorn, and D. Mitton, "RADIUS and IPv6," August 2001.

RFC 3204 Zimmerer, E., J. Peterson, A. Vemuri, L. Ong, F. Audet, M., Watson, and M. Zonoun, "MIME media types for ISUP and QSIG Objects," December 2001.

RFC 3209 Awduche, D., L. Berger, D. Gan, T. Li, V. Srinivasan, and G. Swallow, "RSVP-TE: Extensions to RSVP for LSP Tunnels," December 2001.

RFC 3210 Awduche, D., A. Hannan, and X. Xiao, "Applicability Statement for Extensions to RSVP for LSP-Tunnels," December 2001.

RFC 3246 Davie, B., A. Charny, J.C.R. Bennett, K. Benson, J.Y. Le Boudec, W. Courtney, S. Davari, V. Firoiu, and D. Stiliadis, "An Expedited Forwarding PHB (Per-Hop Behavior)," March 2002.

RFC 3261 Rosenberg, J., H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and R. Schooler, "SIP: Session Initiation Protocol," June 2002.

RFC 3262 Rosenberg, J. and H. Schulzrinne, "Reliability of Provisional Responses in Session Initiation Protocol (SIP)," June 2002.

RFC 3264 Rosenberg, J. and H. Schulzrinne, "An Offer/Answer Model with the Session Description Protocol (SDP)," June 2002.

RFC 3265 Roach, A. B., "Session Initiation Protocol (SIP)-Specific Event Notification," June 2002.

RFC 3266 Olson, S., G. Camarillo, and A. B. Roach, "Support for IPv6 in Session Description Protocol," June 2002.

RFC 3267 Sjoberg, J., M. Westerlund, A. Lakaniemi, and Q. Xie, "Real-Time Transport Protocol (RTP) Payload Format and File Storage Format for the Adaptive Multi-Rate (AMR) and Adaptive Multi-Rate Wideband (AMR-WB) Audio Codecs," June 2002.

RFC 3270 Le Faucheur, F., L. Wu, B. Davie, S. Davari, P. Vaananen, R. Krishnan, P. Cheval, and J. Heinanen, "Multi-Protocol Label Switching (MPLS) Support of Differentiated Services," May 2002.

RFC 3310 Niemi, A., J. Arkko, and V. Torvinen, "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)," September 2002.

RFC 3311 Rosenberg, J., "The Session Initiation Protocol (SIP) UPDATE Method," September 2002.

RFC 3312 Camarillo, G., W. Marshall, and J. Rosenberg, "Integration of Resource Management and Session Initiation Protocol (SIP)," October 2002.

RFC 3315 Droms, E., J. Bound, B. Volz, T. Lemon, C. Perkins, and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)," July 2003.

RFC 3323 Peterson, J., "A Privacy Mechanism for the Session Initiation Protocol (SIP)," November 2002.

RFC 3325 Jennings, C., J. Peterson, and M. Watson, "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks," November 2002.

RFC 3326 Schulzrinne, H., D. Oran, and G. Camarillo, "The Reason Header Field for the Session Initiation Protocol (SIP)," December 2002.

RFC 3329 Arkko, J., V. Torvinen, G. Camarillo, A. Niemi, and T. Haukka, "Security Mechanism Agreement for the Session Initiation Protocol (SIP)," January 2003.

RFC 3331 Morneault, K., R. Dantu, G. Sidebottom, B. Bidulock, and J. Heitz, "Signaling System 7 (SS7) Message Transfer Part 2 (MTP2) – User Adaptation Layer," September 2002.

RFC 3359 Przygienda, T., "Reserved Type, Length and Value (TLV) codepoints in Intermediate System to Intermediate System" August 2002.

RFC 3366 Fairhurst, G., and L. Wood, "Advice to link designers on link Automatic Repeat reQuest (ARQ)," August 2002.

RFC 3372 Vemuri, A., and J. Peterson, "Session Initiation Protocol for Telephones (SIP-T): Context and Architecture," September 2002.

RFC 3398 Camarillo, G., A. B. Roach, J. Peterson, and L. Ong, "Integrated Services Digital Network (ISDN) User Part (ISUP) to Session Initiation Protocol (SIP) Mapping," December 2002.

RFC 3410 Case, J., R. Mundy, D. Partain, and B. Stewart, "Introduction and Applicability Statements for Internet Standard Management Framework," December 2002.

RFC 3411 Harrington, D., R. Presuhn, and B. Wijnen, "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks," December 2002.

RFC 3412 Case, J., D. Harrington, R. Presuhn, and B. Wijnen, "Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)," December 2002.

RFC 3413 Levi, D., P. Meyer, and B. Stewart, "Simple Network Management Protocol (SNMP) Applications," December 2002.

RFC 3414 Blumenthal, U., and B. Wijnen, "User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3), December 2002.

RFC 3415 "View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)"

RFC 3416 Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)"

RFC 3417 "Transport Mappings for the Simple Network Management Protocol"

RFC 3418 "Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)"

RFC 3443 Agarwal, P. and B. Akyol, "Time To Live (TTL) Processing in Multi-Protocol Label Switching (MPLS) Networks," January 2003.

RFC 3455 Garcia-Martin, M., E. Henrikson, and D. Mills, "Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)," January 2003.

RFC 3459 Burger, E., "Critical Content Multi-Purpose Internet Mail Extensions (MIME) Parameter," January 2003.

RFC 3469 Sharma, V. and F. Hellstrand, "Framework for Multi-Protocol Label Switching (MPLS)-Based Recovery," February 2003.

RFC 3471 Berger, L., Ed., "Generalized Multi-Protocol Label Switching (GMPLS) Signaling Functional Description," January 2003.

RFC 3473 Berger, L., Ed., "Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions," January 2003.

RFC 3478 Leelanivas, M., Y. Rekhter, and R. Aggarwal, "Graceful Restart Mechanism for Label Distribution Protocol," February 2003.

RFC 3479 Farrel, A., Ed., "Fault Tolerance for the Label Distribution Protocol (LDP)," February 2003.

RFC 3484 Draves, R., "Default Address Selection for Internet Protocol Version 6 (IPv6)," February 2003.

RFC 3486 Camarillo, G., "Compressing the Session Initiation Protocol (SIP)," February 2003.

RFC 3515 Sparks, R., "The Session Initiation Protocol (SIP) Refer Method," April 2003.

RFC 3550 Schulzrinne, H., S. Casner, R. Frederick, and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications," July 2003.

RFC 3564 Le Faucheur, F. and W. Lai, "Requirements for Support of Differentiated Services-aware MPLS Traffic Engineering," July 2003.

RFC 3569 Bhattacharyya, S., "An Overview of Source-Specific Multicast (SSM)," July 2003.

RFC 3581 Rosenberg, J. and H. Schulzrinne, "An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing," August 2003.

RFC 3584 Frye, R., D. Levi, S. Routhier, and B. Wijnen, "Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework," August 2003.

RFC 3595 Wijnen, B., "Textual Conventions for IPv6 Flow Label," September 2003.

RFC 3596 Thomson, S., C. Huitema, V. Ksinant, and M. Souissi, "DNS Extensions to Support IPv6," October 2003.

RFC 3608 Willis, D., and B. Hoeneisen, "Session Initiation Protocol (SIP) Extension Header Field for Service Route Discovery During Registration," October 2003.

RFC 3618 Fenner, B. and D. Meyer, "Multicast Source Discovery Protocol (MSDP)," October 2003.

RFC 3662 Bless, R., K. Nichols, and K. Wehrle, "A Lower Effort Per-Domain Behavior (PDB) for Differentiated Services," December 2003.

RFC 3670 Moore, B., D. Durham, J. Strassner, A. Westerinen, and W. Weiss, "Information Model for Describing Network Device QoS Datapath Mechanism," January 2004.

RFC 3711 Baugher, M., D. McGrew, M. Naslund, E. Carrara, and K. Norrman, "The Secure Real-time Transport Protocol (SRTP)," March 2004.

RFC 3768 Hinden, R., "Virtual Router Redundancy Protocol (VRRP)," April 2004.

RFC 3775 Johnson, D., C., Perkins, and J. Arkko, "Mobility Support in IPv6," June 2004.

RFC 3776 Arrko, J., V. Devarapalli, and F. Dupont, "Using IPSec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents," June 2004.

RFC 3810 Vida, R., Ed. And L. Costa, Ed., "Multicast Listener Discovery Version 2 (MLDv2) for IPv6," June 2004.

RFC 3826 Blumenthal, U., F. Maino, and K. McCloghrie, "The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model," June 2004.

RFC 3840 Rosenberg, J., H. Schulzrinne, and P. Kyzivat, "Indicating User Agent Capabilities in the Session Initiation Protocol (SIP)," August 2004.

RFC 3853 Peterson, J., "S/MIME Advanced Encryption Standard (AES) Requirements for the Session Initiation Protocol (SIP)," July 2004.

RFC 3868 Loughney, J., Ed., G. Sidebottom, L. Coene, G. Verwimp, J. Keller, and B. Bidulock, "Signalling Connection Control Part User Adaptation Layer (SUA)," October 2004.

RFC 3890 Westerlund, M., "A Transport Independent Bandwidth Modifier for the Session Description Protocol (SDP)," September 2004.

RFC 3891 Mahy, R., B. Biggs, and R. Dean, "The Session Initiation Protocol (SIP) "Replaces" Header," September 2004.

RFC 3892 Sparks, R., "The Session Initiation Protocol (SIP) Referred-By Mechanism," September 2004.

RFC 3913 Thaler, D., "Border Gateway Multicast Protocol (BGMP)," September 2004.

RFC 3920 Saint-Andre, P., Ed., "Extensible Messaging and Presence Protocol (XMPP): Core," October 2004.

RFC 3921 Saint-Andre, P., Ed., "Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence," October 2004.

RFC 3936 Kompella, K. and J. Lang, "Procedures for Modifying the Resource reSerVation Protocol (RSVP)," October 2004.

RFC 3960 Camarillo, G., and H. Schulzrinne, "Early Media and Ringing Tone Generation in the Session Initiation Protocol (SIP)," December 2004

RFC 3963 Devarapalli, V., R. Wakikawa, A. Petrescu, and P. Thurbert, "Network Mobility (NEMO) Basic Support Protocol," January 2005.

RFC 3966 Schulzrinne, H., "The tel URI for Telephone Numbers," December 2004.

RFC 3968 Camarillo, G., "The Internet Assigned Number Authority (IANA) Header Field Parameter Registry for the Session Initiation Protocol (SIP)," December 2004.

RFC 3971 Arkko, E., B. Zill, J. Kempf, and P. Nikander, "Secure Neighbor Discovery (SEND)," March 2005.

RFC 3984 Wenger, S., M. M. Hannuksela, T., Stockhammer, M. Westerlund, and D. Singer, "RTP Payload Format for H.264 Video," February 2005.

RFC 3986 Berners-Lee, T., R. Fielding, and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax," January 2005.

RFC 4003 Berger, L., "GMPLS Signaling Procedure for Egress Control," February 2005.

RFC 4007 Deering, S., B. Haberman, T. Jinmei, E. Nordmark, and B. Zill, "IPv6 Scoped Address Architecture," March 2005.

RFC 4022 Raghunarayan, R., "Management Information Base for the Transmission Control Protocol (TCP)," March 2005.

RFC 4028 Donovan, B., and J. Rosenberg, "Session Timers in the Session Initiation Protocol (SIP)," April 2005.

RFC 4040 Kreuter, R., "RTP Payload Format for a 64 kbit/s Transparent Call," April 2005.

RFC 4087 Thaler, D., "IP Tunnel MIB," June 2005.

RFC 4090 Pan, P., Ed., G. Swallow, Ed., and A. Atlas, Ed., "Fast Reroute Extensions to RSVP-TE for LSP Tunnels," May 2005.

RFC 4091 Camarillo, G. and J. Rosenburg, "The Alternative Network Address Types (ANAT) Semantics for the Session Description Protocol (SDP) Grouping Framework," June 2005.

RFC 4092 Camarillo, G. and J. Rosenburg, "Usage of the Session Description Protocol (SDP) Alternative Network Address Types (ANAT) Semantics in the Session Initiation Protocol (SIP)," June 2005.

RFC 4109 Hoffman, P., "Algorithms for Internet Key Exchange Version 1 (IKEv1)," May 2005.

RFC 4113 Fenner, B. and J. Flick, "Management Information Base for the User Datagram Protocol (UDP)," June 2005.

RFC 4124 Faucheur, F., "Protocol Extensions for Support of Diffserv-aware MPLS Traffic Engineering," June 2005.

RFC 4165 George, T., B. Bidulock, R. Dantu, H. Schwarzbauer, and K. Morneault, "Signaling System 7 (SS7) Message Transfer Part 2 (MTP2) – User Peer-to-Peer Adaptation Layer (M2PA)," September 2005.

RFC 4176 El Mghazli, Y., Ed., T. Nadeau, M. Boucadair, K. Chan, AND A. Gonguet, "Framework for Layer 3 Virtual Private Networks (L3VPN) Operations and Management," October 2005.

RFC 4182 Rosen, E., "Removing a Restriction on the use of MPLS Explicit NULL," September 2005.

RFC 4191 Draves, R. and D. Thaler, "Default Router Preferences and More-Specific Routes," November 2005.

RFC 4193 Hinden, R. and B. Haberman, "Unique Local IPv6 Unicast Addresses," October 2005.

RFC 4201 Kompella, K., Y. Rekhter, and L. Berger, "Link Bundling in MPLS Traffic Engineering (TE)," October 2005.

RFC 4204 Lang, J., "Link Management Protocol (LMP)," October 2005.

RFC 4206 Kompella, K. and Y. Rekhter, "Label Switched Paths (LSP) Hierarchy with Generalized Multi-Protocol Label Switching (GMPLS) Traffic Engineering (TE)," October 2005.

RFC 4213 Nordmark, E. and R. Gilligan, "Basic Transition Mechanisms for IPv6 Hosts and Routers," October 2005.

RFC 4233 Morneault, K., S. Rengasami, M. Kalla, and G. Sidebottom, "Integrated Services Digital Network (ISDN) Q.921-User Adaptation Layer, January 2006.

RFC 4251 Ylonen, T., and C. Lonvick, Ed., "The Secure Shell (SSH) Protocol Architecture," January 2006.

RFC 4252 Ylonen, T., and C. Lonvick, Ed., "The Secure Shell (SSH) Authentication Protocol," January 2006.

RFC 4253 Ylonen, T., and C. Lonvick, Ed., "The Secure Shell (SSH) Transport Layer Protocol," January 2006.

RFC 4254 Ylonen, T., and C. Lonvick, Ed., "The Secure Shell (SSH) Connection Protocol," January 2006.

RFC 4271 Rekhter, Y., T. Li, and S. Hares, "A Border Gateway Protocol 4 (BGP-4)," January 2006.

RFC 4282 Aboba, B., M. Beadles, J. Arkk and P. Eronen, "The Network Access Identifier," December 2005.

RFC 4291 Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture," February 2006.

RFC 4292 Haberman, B., "IP Forwarding Table MIB," April 2006.

RFC 4293 Routhier, S., "Management Information Base for the Internet Protocol (IP)," April 2006.

RFC 4294 Loughney, E., "IPv6 Node Requirements," April 2006.

RFC 4295 Keeni, G., K. Koide, K. Nagami, and S. Gundavelli, "Mobil IP Management Management Information Base (MIB)," April 2006.

RFC 4301 Kent, S. and K. Seo, "Security Architecture for the Internet Protocol," December 2005.

RFC 4302 Kent, S., "IP Authentication Header," December 2005.

RFC 4303 Kent, S., "IP Encapsulating Security Payload (ESP)," December 2005.

RFC 4304 Kent, S., "Extended Sequence Number (ESN) Addendum to IPSec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP)," December 2005.

RFC 4305 Eastlake, D., "Cryptographic Algorithm Implementation Requirements for the Encapsulating Security Payload (ESP) and Authentication Header (AH)," December 2005.

RFC 4306 Kaufman, E., "Internet Key Exchange (IKEv2) Protocol," December 2005.

RFC 4307 Schiller, J., "Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)," December 2005.

RFC 4308 Hoffman, P., "Cryptographic Suites for IPSec," December 2005.

RFC 4320 Sparks, R., "Action Addressing Identified Issues with the Session Initiation

RFC 4328 Papadimitriou, D., Ed., "Generalized Multi-Protocol Label Switching (GMPLS) Signaling Extensions for G.709 Optical Transport Networks Control," January 2006.

RFC 4330 Mills, D., "Simple Network Time Protocol (SNTP) version 4 for IPv4, IPv6, and OSI," January 2006.

RFC 4364 Rosen, E. and Y. Rekhter, "BGP/MPLS IP Virtual Private Networks (VPNs)," February 2006. (Replaces RFC 2547)

RFC 4379 Kompella, K. and G. Swallow, "Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures," February 2006.

RFC 4382 Nadeau, T., Ed., and H. van der Linde, Ed., "MPLS/BGP Layer 3 Virtual Private Network (VPN) Management Information Base," February 2006.

RFC 4411 Polk, J., "Extending the Session Initiation Protocol (SIP) Reason Header for Preemption Events," February 2006.

RFC 4412 Schulzrinne, H. and J. Polk, "Communications Resource Priority for the Session Initiation Protocol (SIP)," February 2006.

RFC 4420 Farrel, A., Ed., D. Papadimitriou, J.P. Vasseur, and A. Ayyangar, "Encoding of Attributes for Multiprotocol Label Switching (MPLS) Label Switched Path (LSP) Establishment Using Resource ReserVation Protocol-Traffic Engineering (RSVP-TE)," February 2006.

RFC 4422 Melnikov, E., Zeilenga, E., "Simple Authentication and Security layer (SASL)," June 2006.

RFC 4443 Conta, A., S. Deering, and M. Gupta, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification," March 2006.

RFC 4447 Martini, L., Ed., E. Rosen, N. El-Aawar, T. Smith, and G. Heron, "Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)," April 2006.

RFC 4448 Martini, L., Ed., E. Rosen, N. El-Aawar, and G. Heron, "Encapsulation Methods for Transport of Ethernet over MPLS Networks," April 2006.

RFC 4456 Bates, T., Chen, E., "BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP)," April 2006.

RFC 4510 Zeilenga, E., "Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map," June 2006.

RFC 4511 Sermersheim, J., "Lightweight Directory Access Protocol (LDAP): The Protocol," June 2006.

RFC 4552 Gupta, M. and N. Melam, "Authentication/Confidentiality for OSPFV3," June 2006.

RFC 4566 Handley, M., V. Jacobson, and C. Perkins, "SDP: Session Description Protocol," July 2006.

RFC 4568 Andreasen, F., M. Baugher, and D. Wing, "Session Description Protocol (SDP) Security Descriptions for Media Streams," July 2006.

RFC 4573 Even, R., and A. Lochbaum, "MIME Type Registration for RTP Payload Format for H.224," July 2006.

RFC 4574 Levin, O., and G. Camarillo, "Session Description Protocol (SDP) Label Attribute," August 2006.

RFC 4582 Camarillo, G., J. Ott, and K. Drage, "The Binary Floor Control Protocol (BFCP)," November 2006.

RFC 4583 Camarillo, G., "Session Description Protocol (SDP) Format for Binary Floor Control Protocol (BFCP) Streams," November 2006.

RFC 4585 Ott, J., S. Wenger, N. Sato, C. Burmeister, and J. Rey, "Extended RTP Profile for Real-time Transport Control Protocol (RTCP)-Based Feedback (RTP/AVPF), July 2006.

RFC 4604 Holbrook, H., Haberman, B. and B. Cain, "Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery protocol Version 2 (MLDv2) for Source-Specific Multicast," August 2006.

RFC 4607 Holbrook, H. and B. Cain, "Source-Specific Multicast for IP," August 2006.

RFC 4659 De Clercq, J., D. Ooms, M. Carugi, and F. Le Faucheur, "BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN," September 2006.

RFC 4666 Morneault, K., Ed., and J. Pastor-Balbas, Ed., "Signaling System 7 (SS7) Message Transfer Part 3 (MTP3) – User Adaptation Layer (M3UA)," September 2006.

RFC 4684 Marques, P., R. Bonica, L. Fang, L. Martini, R. Raszuk, K. Patel, and J. Guichard, "Constrained Route Distribution for Border Gateway Protocol/MultiProtocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs)," November 2006.

RFC 4724 Sangli, S., Chen, E., Fernando, R., Scudder, J., Rekhter, Y., "Graceful Restart Mechanism for BGP," January 2007.

RFC 4730 "A SIP Event Package for Key Press Stimulus."

RFC 4733 "RTP Payload for DTMF Digits, Telephony Tones, and Telephony Signals."

RFC 4760 Bates, T., R. Chandra, D. Katz and Y. Rekhter, "Multiprotocol Extensions for BGP-4," January 2007.

RFC 4761 Kompella, K., Ed. and Y. Rekhter, Ed., "Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling," January 2007. (Updated by RFC 5462)

RFC 4762 Lasserre, M., Ed. and V. Kompella, Ed., "Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling," January 2007.

RFC 4783 Berger, L., Ed., "GMPLS – Communication of Alarm Information," December 2006.

RFC 4796 Hautakorpi, J. and G. Camarillo, "The Session Description Protocol (SDP) Content Attribute," February 2007.

RFC 4807 Baer, M., R. Charlet, W. Hardaker and R. Story, "IPSec Security Policy Dtabase Configuration MIB," March 2007.

RFC 4835 Manral, V., "Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)," April 2007.

RFC 4861 Narten, T., E. Nordmark, W. Simpson, and H. Soliman, "Neighbor Discovery for IP Version 6 (IPv6)," September 2007.

RFC 4862 Thomson, S., T. Narten, and T. Jinmei, "IPv6 Stateless Address Autoconfiguration," September 2007.

RFC 4869 Law, L. and J. Solinas, "Suite B Cryptographic Suites for IPsec," May 2007.

RFC 4872 Lang, J.P., Ed., Y. Rekhter, Ed., and D. Papadimitriou, Ed., "RSVP-TE Extensions in Support of End-to-End Generalized Multi-Protocol Label Switching (GMPLS) Recovery," May 2007.

RFC 4873 Berger, L., I. Bryskin, D. Papadimitriou, and A. Farrel, "GMPLS Segment Recovery," May 2007.

RFC 4874 Lee, C.Y., A. Farrel, and S. De Cnodder, "Exclude Routes – Extension to Resource ReserVation Protocol-Traffic Engineering (RSVP-TE)," April 2007.

RFC 4877 Devarapalli, V. and F. Dupont, "Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture," April 2007.

RFC 4904 Gurbani, V. and C. Jennings, "Representing Trunk Groups in tel/sip Uniform Resource Identifiers (URIs)," June 2007.

RFC 4941 Narten, T., R. Draves, and S. Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6," September 2007.

RFC 4960 Steewart, E., "Stream Control Transmission Protocol," September 2007.

RFC 4974 Papadimitriou, D. and A. Farrel. "Generalized MPLS (GMPLS) RSVP-TE Signaling Extensions in Support of Calls," August 2007.

RFC 5059 Bhaskar, N., Gall, A., Lingard, J., and S. Venaas, "Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)," January 2008.

RFC 5063 Satyanarayana, A., Ed. and R. Rahman, Ed.. "Extensions to GMPLS Resource Reservation Protocol (RSVP) Graceful Restart," October 2007.

RFC 5065 Traina, P., McPherson, D. and J. Scudder, "Antonomous system Confederations for BGP," August 2007.

RFC 5072 Varada, S., "IP Version 6 over PPP," September 2007.

RFC 5095 Abley, J., P. Savola, and G. Neville-Neil, "Deprecation of Type 0 Routing Headers in IPv6," December 2007.

RFC 5104 Wenger, S., U. Chandra, M. Westerlund, and B. Burman, "Codec Control Messages in the RTP Audio-Visual Profile with Feedback (AVPF)," February 2008.

RFC 5129 Davie, B., B. Briscoe, and J. Tay. "Explicit Congestion Marking in MPLS," January 2008.

RFC 5151 Farrel, A., Ed., A. Ayyangar, and J.P. Vasseur, "Inter-Domain MPLS and GMPLS Traffic Engineering – Resource Reservation Protocol-Traffic Engineering (RSVP-TE) Extensions," February 2008.

RFC 5301 McPherson, D. and N. Shen, "Dynamic Hostname Exchange Mechanism for IS-IS," October 2008.

RFC 5303 Katz, D., Saluja, R. and D. Eastlake, "Three-Way Handshake for IS-IS Point-to-Point Adjacencies," October 2008.

RFC 5304 Li, T. and R. Atkinson, "IS-IS Cryptographic Authentication," October 2008.

RFC 5305 Li, T., Redback Networks, Inc., H. Smit, "IS-IS Extensions for Traffic Engineering," October 2008.

RFC 5306 Shand, M., and L. Ginsberg, “Restart Signaling for IS-IS,” October 2008.

RFC 5307 Kompella, K. and Y. Rekhter, “IS-IS Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS),” October 2008.

RFC 5308 Hopps, C., “Routing IPv6 with IS-IS,” October 2008.

RFC 5309 Shen, N. and A. Zinin, “Point-to-Point Operation over LAN in Link State Routing Protocols,” October 2008.

RFC 5310 Bhatia, M., Manral, V., Li, T., Atkinson, R., White, R. and M. Fanto., “IS-IS Generic Cryptographic Authentication,” February 2009.

RFC 5331 Aggarwal, R., Y. Rekhter, and E. Rosen, “MPLS Upstream Label Assignment and Context-Specific Label Space,” August 2008.

RFC 5332 Eckert, T., E. Rosen, Ed., R. Aggarwal, and Y. Rekhter. “MPLS Multicast Encapsulations,” August 2008.

RFC 5340 Coltun, R., Ferguson, D., Moy, J. and E. Lindem, “OSPF for IPv6,” July 2008.

RFC 5359 Johnston, A., Sparks, R., Cunningham, C., Donovan, S. and K. Summers, “Session Initiation Protocol Service Examples,” October 2008.

RFC 5420 Farrel, A., Ed., D. Papadimitriou, J.P. Vasseur, and A. Ayyangarps, “Encoding of Attributes for MPLS LSP Establishment Using Resource Reservation Protocol Traffic Engineering (RSVP-TE),” February 2009.

RFC 5462 Andersson L. and R. Asati, “Multiprotocol Label Switching (MPLS) Label Stack Entry: "EXP" Field Renamed to "Traffic Class" Field,” February 2009.

RFC 5492 Scudder, J. and R. Chandra, “Capabilities Advertisement with BGP-4” February 2009.

RFC 5501 Kamite, y., Ed., Y. Wada, Y. Serbest, T. Morin, and L. Fang, “Requirements for Multicast Support in Virtual Private LAN Services,” March 2009.

RFC 5503 Marshall, W., Ed., and F. Andreasen, Ed., “Private Session Initiation Protocol (SIP) Proxy-to-Proxy Extensions for Supporting the PacketCable Distributed Call Signaling Architecture,” October 2003.

RFC draft Harrison, J., J. Berger, M. Bartlett, Data Connection Ltd (DCL), draft-ietf-isis-ipv6-te, "IPv6 Traffic Engineering in IS-IS," September 2009, expires March 2010.

A4.13 JOINT REQUIREMENTS OVERSIGHT COUNCIL DOCUMENTATION

JROCM 048-96 Memorandum for the Under Secretary of Defense for Acquisition and Technology, Subject: Validation of Defense Information Systems Network (DISN) Capstone Requirements Document (CRD), 15 April 1996.

JROCM 134-01 "Global Information Grid (GIG) Capabilities Requirement Document (CRD)," 30 August 2001.

JROCM 202-02 "Global Information Grid (GIG), Mission Area Initial Capabilities Document (MA ICD)," 22 November 2002.

A4.14 NATIONAL SECURITY AGENCY DOCUMENTATION

National Security Agency, "Common Criteria for Information Technology Evaluation, Protection Profile for Switches and Routers," Draft 2.1, 22 February 2001.

National Security Agency, "DoD Class 3 Public Key Infrastructure Interface Specification," Version 1.2, 10 August 2000.

A4.15 NATIONAL SECURITY TELECOMMUNICATIONS AND INFORMATION SYSTEMS SECURITY DOCUMENTATION

NSTISSI No. 4009 National Security Telecommunications and Information Systems Security Instruction, "National Information Systems Security (INFOSEC) Glossary," 5 June 1992.

National Security Telecommunications and Information Systems Security Authority Manual (NSTISSAM), "TEMPEST/2-95, RED/Black Installation Guidance," 12 December 1995.

National Security Telecommunications and Information Systems Security Committee (NSTISSC), "National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11, Subject: National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products," January 2000 and revised June 2003.

A4.16 U. S. SECURE COMMUNICATION INTEROPERABILITY PROTOCOL

SCIP-215 U.S. Secure Communication Interoperability Protocol (SCIP) over IP Implementation Standard and Minimum Essential Requirements (MER) Publication, Revision 2.0, 3 October 2007.

SCIP-216 Minimum Essential Requirements (MER) for V.150.1 Gateways Publication, Revision 2.0, 2 November 2007.

A4.17 TELCORDIA TECHNOLOGIES DOCUMENTATION

Feature Service Description (FSD) 30-33-0000, *Release to Pivot Network Capability*.

FR-E911-1 *Requirements to Support E9-1-1 Service*, Issue 5, January 2007.

FR-796 *Reliability and Quality Generic Requirements (RQGR)*, Issue 1, October 1995; Issue 2; Issue 3, March 2006; Issue 5, April 2008.

GR-25-CORE .

GR-63-CORE *NEBS™ Requirements: Physical Protection*, Issue 1, October 1995, Issue 2, April 2002, Issue 3, March 2006.

GR-217-CORE *LSSGR: CLASS^{SM} Feature: Selective Call Forwarding (FSD-01-02-1410)*, Issue 1, June 2000; Issue 2, April 2002.

~~GR-218-CORE *CLASS^{SM} Feature: Selective Call Rejection (FSD 01-02-0760),* Issue 1, June 2000, Issue 2, April 2002.~~

GR-246-CORE *Specification of Signalling System Number 7*, 2005/12/30.

GR-253-CORE *Synchronous Optical Network (SONET) Transport Systems: Common Generic Criteria*, December 2005.

GR-282-CORE *Software Reliability and Quality Acceptance Criteria (SRQAC)*, Issue 3, December 1996.

GR-303-CORE *Integrated Digital Loop Carrier System Generic Requirements, Objectives, and Interface*, Issue 4, December 2000.

GR-317-CORE *Switching System Generic Requirements for Call Control Using the Integrated Services Digital Network User Part (ISDNUP)*, November 2007.

GR-383-CORE *COMMON LANGUAGE® Equipment Codes (CLEI™ Codes) – Generic Requirements for Product Labels*, Issue 3, February 2006.

GR-394-CORE *Switching System Generic Requirements for Interexchange Carrier Interconnection (ICI) Using the Integrated Services Digital Network User Part (ISDNUP)*, November 2007.

GR-436-CORE *Digital Network Synchronization Plan*, Issue 1 with Revision 1, June 1996.

GR-472-CORE *Network Element Configuration Management*, Revision 2, February 1999.

GR-474-CORE OTGR Section 4: *Network Maintenance: Alarm and Control for Network Elements*, December 1997.

GR-477-CORE *Network Traffic Management*, February 2000.

GR-478-CORE *Measurements and Data Generation*, Issue 4, February 2000.

GR-496-CORE *SONET Add-Drop Multiplexer (SONET ADM) Generic Criteria*, Issue 2, August 2007.

GR-499-CORE *Transport Systems Generic Requirements (TSGR): Common Requirements*, Issue 3, September 2004.

GR-505-CORE *Call Processing*, December 1997.

GR-506-CORE *LSSGR: Signaling for Analog Interfaces*, December 2006.

GR-507-CORE *LSSGR: Transition Section 7*, January 2000.

~~GR-510-CORE *System Interfaces*, Issue 1, June 2000.~~

GR-512-CORE *LSSGR: Reliability*, Section 12, January 1998.

GR-513-CORE *Module of the LSSGR, FR-64*, Issue 1, September 1995.

~~GR-517-CORE *LSSGR: Traffic Capacity and Environment*, December 1997.~~

GR-518-CORE *LSSGR: Synchronization Section 18,* Issue 1, May 1994.

~~GR-520-CORE *Features Common to Residence and Business,* Issue 1, June 2000.~~

~~GR-523-CORE *Synchronous Optical Network (SONET) Transport, Issue 3, September 2000, Issue 4, December 2005.*~~

~~GR-524-CORE *LSSGR: Attendant and Customer Switching System Features and Customer Interfaces, PBX Line,* Issue 1, FSD 04-01-0000, June 2000.~~

GR-529-CORE *LSSGR: Public Safety,* Issue 1, FSD 15-03-0000, June 2000.

GR-533-CORE *LSSGR: Database Services – Service Switching Points, Toll-Free Service,* (FSD 31-01-000), June 2001.

~~GR-540-CORE *LSSGR: Tandem Supplement,* Issue 2, March 1999.~~

~~GR-562-CORE *Manual Line Features,* Issue 1, June 2000.~~

~~GR-569-CORE *Multiline Hunt Service,* Issue 1, June 2000.~~

GR-571-CORE *LSSGR: Call Waiting, FSD 01-02-1201*, June 2000.

GR-572-CORE *LSSGR: Cancel Call Waiting, FSD 01-02-1204*, June 2000.

~~GR-577-CORE *Three-Way Calling,* Issue 1, June 2000.~~

~~GR-579-CORE *Add-on Transfer and Conference Calling Features,* Issue 1, June 2000.~~

GR-580-CORE *LSSGR: Call Forwarding Variable, FSD 01-02-1401*, June 2000.

GR-586-CORE *LSSGR: Call Forwarding Subfeatures, FSD 01-02-1450*, April 2002.

GR-590-CORE *LSSGR: Call Pickup Features,* Issue 1, June 2000.

GR-606-CORE *LSSGR: Common Channel Signaling, Section 6.5,* Component of FR-64, December 2004.

~~GR-690-CORE *LSSGR: Exchange Access Interconnection,* FSD 20-24-0000, November 1996.~~

~~GR-741-CORE~~ ~~*LSSGR: Network Administration Center (NAC) Input/Output (I/O) Channel*, FSD 45-10-0000, June 2000.~~

~~GR-747-CORE~~ ~~*LSSGR: An Alternative Implementation of an SPCS to NTM OS Interface via an NDC OS*, FSD 45-18-0450, June 2000.~~

GR-740-CORE *Stored Program Control System/Operations System (SPCS/OS) - Network Data Collection Operations System (NDC OS) Interface*, , March 200).

GR-782-CORE *SONET Digital Switch Trunk Interface Criteria*, A Module of TSGR, FR-440, Issue 1, June 2000 (Formerly TR-TSY-000782, Issue 2, September 1989).

GR-815-CORE *Generic Requirements for Network Element/Network System (NE/NS) Security: A Module of LSSGR*, Component of FR-64, Issue 2, March 2002.

GR-820-CORE *OTGR Section 5.1: Generic Digital Transmission Surveillance*, Issue 2, December 1997.

~~GR-822-CORE~~ ~~*OTGR Section 6.3: Network Maintenance: Access and Testing Switched Circuits, Pots Loops and Public Packet Switched Network (PPSN),* December 1995.~~

~~GR-844-CORE~~ ~~*Network Maintenance: Access and Testing TSC/RTU Generic Requirements for Metallic Loop Testing*, November 1995.~~

GR-874-CORE *An Introduction to the Reliability and Quality Generic Requirements (RQGR)*, Issue 3, April 1997.

GR-957-CORE *Optical Interfaces for Equipment and Systems Relating to the Synchronous Digital Hierarchy)*, 2006.

GR-1089-CORE *Electromagnetic Compatibility and Electrical Safety - Generic Criteria for Network Telecommunications Equipment*, Issue 05, August 2009.

GR-1100-CORE *Billing Automatic Message Accounting Format (BAF) Generic Requirements*, December 2007.

GR-1230-CORE *SONET Bi-Directional Line-Switched Ring Equipment Generic Criteria*, Issue 4, December 1998.

GR-1244-CORE *Clocks for the Synchronized Network: Common Generic Criteria*, Issue 1, May 2005.

GR-1400-CORE *SONET Unidirectional Path Switched Ring (UPSR) Equipment Generic Criteria*, Issue 3, July 2006.

GR-2911-CORE *Software Inventory for Network Element Software Management*, Issue 1, June 1995.

GR-2932-CORE *Database Functionalities*, May 1997.

GR-2996-CORE *Generic Criteria for SONET Digital Cross-Connect Systems*, Issue 1, January 1999.

GR-3051-CORE *Voice Over Packet: NGN Call Connection Agent Generic Requirements*, Issue 2, January 2001.

~~GR-3053-CORE *Voice Over Packet (VOP): Next Generation Network (NGN) Signaling Gateway Generic Requirements*, February 2000.~~

GR-3054-CORE *Voice Over Packet: NGN Trunk Gateway Generic Requirements*, Issue 1, March 2000.

GR-3055-CORE *Voice Over Packet: NGN Access Gateway Generic Requirements*, Issue 1, March 2000.

GR-3058-CORE *Voice over Packet (VoP): Next Generation Networks (NGN) Accounting Management Generic Requirements*, December 2005.

SR-2275 *Telcordia Notes on the Networks*, Issue 4, October 2000.

SR-3476 *National ISDN 1995 and 1996*, Issue 1, June 1995.

SR-3580 *NEBS Criteria Levels*, Issue 3, June 2007.

SR-4994 *2000 Version of National ISDN Primary Rate Interface (PRI) Customer Premises Equipment Generic Guidelines*, Issue 1, December 1999.

SR-NWT-002120 *National ISDN-2*, Issue 1, May 1992 with revision 1, June 1993.

SR-NWT-002343 *ISDN Primary Rate Interface Generic Guidelines for Customer Premises Equipment*, Issue 1, June 1993.

SR-NWT-002419 *Software Architecture Review Checklists*, Issue 01, December 1992.

TR-917 *SONET Regenerator (SONET RGTR) Equipment Generic Criteria*, December 1990.

TR-NWT-000057 *Functional Criteria for Digital Loop Carrier Systems*, Issue 2, January 1993.

TR-NWT-000179 *Software Quality Program Generic Requirements*, June 1993.

TR-NWT-000284 *Reliability and Quality Switching Systems Generic Requirements (RQSSGR)*, Issue 2, October 1990.

TR-NWT-000295 *Isolated Ground Planes: Definition and Application to Telephone Central Offices*, Issue 2, July 1992.

TR-NWT-000418 *Generic Reliability Assurance for Fiber Optic Transport Systems*, Issue 2, December 1992.

TR-NWT-001244 *Clocks for the Synchronized Network: Common Generic Criteria*, Issue 1, June 1993.

TR-NWT-001268 *ISDN Primary Rate Interface Call Control Switching and Signaling Generic Requirements for Class II Equipment*, Issue 1, December 1991.

Telcordia and Computer Sciences Corporation, *Call Connection Agent (CCA) Chapter, Assured Real Time Service (ARTS) Generic System Requirement (GRS)*, Draft October 2006.

Telcordia and Computer Sciences Corporation, *Media Gateway Chapter, Assured Real Time Service (ARTS) Generic System Requirement (GRS)*, Draft October 2006.

Telcordia and Computer Sciences Corporation, *Signaling Gateway Chapter, Assured Real Time Service (ARTS) Generic System Requirement (GRS)*, Draft October 2006.

A4.18 UNITED STATES CODE

Title 10 Section 2224, "Defense Information Assurance Program."
Title 40 Section 11331.
Title 44 "Federal Information Security Management Act (FISMA) of 2002."

A4.19 OTHER DOCUMENTATION

3G TS 24.067 V3.0.0 (1999-05), 3rd Generation Partnership Project; Technical Specification Group Core Network; enhanced MLPP (eMLPP) – Stage 3.

ASD(NII)/DoD CIO Memorandum, "Department of Defense Unified Capabilities Requirements," current edition.

ASD(NII)/DoD CIO, "Global Information Grid (GIG) Architectural Vision."

ASD(NII)/DoD CIO, "DoD Unified Capabilities 2008 (UCR 2008)," January 2009.

ASD(NII)/DoD CIO, "DoD Unified Capabilities 2008 (UCR 2008) Change 1", January 2010.

ATIS-PP-1000012.2006, Signaling Systems No. 7 (SS7) – SS7 – Network and NNI Interconnection Security Requirements and Guidelines, November 2006.

DCID 6/3, Series, "Protecting Sensitive Compartmented Information within Information Systems."

EIA-310C, "19-inch rack mounting equipment specification."
EIA/TIA-232-E, "Interface Between Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange," (superseded by TIA-232-F), January 1991.

EIA-366-A, "Interface Between Data Terminal Equipment and Automatic Calling Equipment for Data Communication."

EIA-449-1, "General Purpose 37-Position and 9-Position Interface for Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange," January 2000.

Federal Telecommunications Recommendation 1080B-2002, *"Video Teleconferencing Services,"* August 15, 2002.

"Generic Cryptographic Interoperability Requirements Document (GCIRD)," Version 1.3, January 7, 2008.

Global Information Grid (GIG) Mission Area Initial Capabilities Document, (MA ICD), 6 January 2003.

House Report 107-436, "Bob Stump National Defense Authorization Act for Fiscal Year 2003": Report of the Committee on Armed Services, House of Representatives on H.R. 4546, 3 May 2002.

International Electrotechnical Commission (IEC), 60950-1, "Information technology equipment – Safety – Part 1: General requirements," Second Edition, 2005-12.

Joint Interoperability Test Center, "Internet Protocol Version 6 Generic Test Plan," Version 2, June 2006.

Joint Staff, Command, Control, Communications, and Computer Systems Directorate (J-6), "Joint Net-Centric Operations Campaign Plan," October 2006.

Joint Staff, "Global Information Grid 2.0 (GIG 2.0) Concept of Operations (CONOPS)."

Joint Staff, "Global Information Grid 2.0 (GIG 2.0) Initial Capability Document (ICD)."

Joint Staff, "Global Information Grid 2.0 (GIG 2.0) Implementation Plan."

National Communications System, NCS Directive 3-10, "Telecommunications Operations, Government Emergency Telecommunications Service (GETS)," 2000.

~~Net-Centric I Document (NCID) Version 3 QoS (T300).~~

North American Treaty Organization (NATO), Standard NATO Agreement (STANAG 4214), "International Rating and Directory for Tactical Communications Systems," Edition 3, Version T, 07 January 2005.

Office of Management and Budget (OMB) Circular A-130, Appendix III.

Public Law 107-314, Section 353, "Bob Stump National Defense Authorization Act for Fiscal Year 2003," 2 December 2002.

Real-Time Services Information Assurance Working Group, "Analysis of IA Requirements and Threats for the DoD RTS Environment," Version 2.2, July 2005.

Real-Time Services Working Group, "Real Time Services (RTS) Information Assurance (IA) Generic System Requirements (GSR)," Version 1.3, 6 July 2006.

Reference Guide for Nodal Manager, "ESOP and Global Edition," Version 4.0, January 1998.

TIA-232-F, "Interface Between Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange."

TIA-422-B, "Electrical Characteristics of Balanced Voltage Digital Interface Circuits," (ANSI/TIA/EIA-422-B-1994) (R2000) (R2005), April 13, 2004.

TIA-530-A, "High Speed 25-Position Interface for Data Terminal Equipment and Data Circuit-Terminating Equipment, Including Alternative 26-Position Connector," ANSI/TIA/EIA-530-A-92) (R98) (R2003), June 1992.

TIA/EIA-470-B, "Telecommunications - Telephone Terminal Equipment - Performance and Compatibility Requirements for Telephone Sets with Loop Signaling," 1997.

TIA TSB-116, "Telecommunications – IP Telephony Equipment – Voice Quality Recommendations for IP Telephony," March 2001.

TIA TSB-116-A, "Telecommunications System Bulletin – Telecommunications – IP Telephony Equipment – Voice Quality Recommendations for IP Telephony," March 2006.

TM 11-5805-681-12 series, "Operator's and Organizational Maintenance Manual for Central Office, Telephone, Automatic AN/TTC-39(V)2."

Underwriters Laboratories, Inc., UL-1950, Standard for Safety, Information Technology Equipment Including Electrical Business Equipment," First Edition, 1999.

"Wireless Priority Service (WPS) Industry Requirements for the Full Operating Capability (FOC) for CDMA-Based Systems – Home Location Register (HLR)," Issue 1, 04 June 2004.

"Wireless Priority Service (WPS) Industry Requirements for the Full Operating Capability (FOC) for GSM-Based Systems," Issue 2, January 2004.

THIS PAGE INTENTIONALLY LEFT BLANK